PLC网络系统配置指南

WANGLUO XITONG PEIZHI ZHINAN

宋伯生 编著





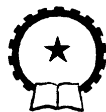
机械工业出版社
CHINA MACHINE PRESS

VISIT…

LANZAROTE
Caliente.com

PLC网络系统配置指南

宋伯生　编著



机 械 工 业 出 版 社

本书先简要介绍PLC网络的基础知识，进而围绕PLC串口网络、设备网络、控制网络和信息网络，对AB、OMRON、西门子、三菱及和利时等厂家PLC使用的、有公认标准可依的这些网络的组成、协议、功能、规格及特点作了分析，并以典型应用配置为实例，介绍了这些网络组态的具体步骤。本书是作者继出版《PLC编程理论、算法及技巧》等多部PLC专著之后的一本针对PLC网络系统配置的专著。本书的内容完整、涉及面广、信息量大、指导性强。相比已有其他介绍PLC网络的专著，像本书这样抓住PLC网络的当今主流，把握PLC网络的发展趋势，从网络机理到应用配置作这么系统的说明，对各个品牌PLC网络作这么全面的介绍，似乎还未曾有过。本书既可帮助您了解当今流行的PLC网络概貌，又可作为您进行PLC网络配置与组态的向导，进而还能使您成为精通多品牌PLC网络、熟悉网络系统配置的高手。

本书可作为有关PLC培训班及高校进行PLC网络教学的参考教材，也可作为全面学习PLC网络技术的自学用书，还可作为PLC网络设计及使用部门技术人员及有关论文撰写者的参考文献。

图书在版编目（CIP）数据

PLC网络系统配置指南/宋伯生编著. —北京：机械工业出版社，2011.5

ISBN 978-7-111-34132-1

Ⅰ.①P… Ⅱ.①宋… Ⅲ.①可编程序控制器—程序设计 Ⅳ.①TP332.3

中国版本图书馆CIP数据核字（2011）第063498号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
策划编辑：罗 莉 责任编辑：罗 莉 版式设计：张世琴
责任校对：樊钟英 封面设计：陈 沛 责任印制：杨 曦
保定市中画美凯印刷有限公司印刷
2011年7月第1版第1次印刷
184mm× 2 60mm·26.5 印张·654
千字0001— 3000册
标准书号：ISBN 978-7-111-34132-1
定价 :69.80元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销 售 一 部：（010）68326294
销 售 二 部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com

封面无防伪标均为盗版

前　　言

PLC 网络的广泛应用是进入 21 世纪以来 PLC 技术进步的重要标志。PLC 连网已是当今 PLC 硬件的必要配置。正是 PLC 网络的广泛应用，PLC 控制系统已越来越成为工厂信息系统不可分割的组成部分，再也不是孤立的“信息孤岛”。可以这么说，当今已是“无 PLC 不连网”，差别只是连的是什么网络，以及是常态连网还是临时连网。试想，当今 PLC 不连网怎么编程？不编程又怎么能工作？

处理 PLC 连网有两个基本问题要解决好：一是系统配置，二是通信编程。前者是组建（设计、采购、安装）网络与配置（设置、组态）网络，为后者提供平台。后者要使网络正常运转，实现站点间数据交换、信息交流，达到连网的目的。这两者缺一不可，但各有各的着重点。一般来讲，从事系统集成的更重视前者，总要尽量把网络组建好。而网络使用人员则更关心后者，力求使组建好的网络为控制优化与信息交流所用。本书着重介绍系统配置，至于通信编程将另有专著介绍。

本书共 5 章。之前还有简短的绪论。由于至今对 PLC 网络还没有公认的定义，所以，在此先对本书要讨论的 PLC 网络的有关概念做一些介绍，以便理解后续章节的内容。

本书第 1 章介绍 PLC 网络基础知识。从技术的基本点上讲，PLC 网络与计算机网络是完全相同的。所以，本章介绍的 PLC 网络基础知识也包含有很多计算机网络的知识。此外，本章还对 PLC 网络的概况及通信实现作了说明。

第 2 章介绍 PLC 串口网络配置。先是介绍串口常用标准，继而介绍各种常用品牌 PLC 的串口特点及网络配置实例。串口网络虽是最简单、最基本，也是 PLC 使用最早、最常见的网络。但它的技术也在发展，功能也在增加。通过串口，实现计算机、人机界面与 PLC 连网、通信是最廉价，也是最方便的。在相同品牌 PLC 之间，使用它很容易连网，并可实现多种方式的数据交换与相互操作。在不同品牌 PLC 之间，如必要，也可对其中一个串口做适当转换便可连网，并利用好相关通信指令也可通信。至于现场设备，只要配置有串口，PLC 也可与其连网、通信。所以，本书介绍 PLC 网络首先对串口网络做了较详细的说明。

第 3 章介绍 PLC 设备网配置。PLC 设备网是用以实现 PLC 与地处远程的操作器、传感器这样的底层工业设备通信的网络，是 PLC 实现远程分布控制的基础，已用得越来越多。考虑到这类网络的普及情况及发展前景，这里主要介绍 AS－i、CC－Link/LT 及 CompoNet3 种开放的标准设备网络。

第 4 章介绍 PLC 控制网配置。PLC 控制网主要用于 PLC 站点间的数据交换与相互操作，也可用于 PLC 对远程设备的控制，既是 PLC 最重要的网络，也是 PLC 实现控制网络化的基础。特别是随着 PLC 控制地域的扩展，控制规模的扩大，其应用也越来越多。

过去 PLC 控制网络多是专有的，一家一个样，而如今已有了很多公认的开放标准网络。而且，有实力的 PLC 厂家的新机型多在使用自身专有控制网络的同时，也逐步与开放网络标准兼容。一些 PLC 厂家，如和利时、ABB 公司干脆就直接采用这些标准，以使自身的产品可以加入这些网络，从而扩展自身产品的应用。为此，本书在介绍 PLC 控制网络时，就只介绍几个流行的开放标准网络，具体是 CC-Link、DeviceNet、ControlNet 及 Profibus 等。

第 5 章介绍 PLC 信息网配置。当今 PLC 信息网用的几乎全是以太网。这与以太网的技术优势、发展快速与应用广泛有关。原先 PLC 以太网主要是用于与企业高层计算机连网。但由于工业以太网的出现，其环境的适应性、通信的实时性及信息的安全性都有极大进步，已使它也可用于 PLC 间的链接数据及与分布设备间的 I/O 数据的实时交换，以至于进一步发展还可用于安全与运动控制。如 AB 公司等开发的 EtherNet/IP/西门子公司等开发的 Profinet 及三菱公司等开发的 CC-Link IE 等工业以太网就已经或即将实现这些目标。人们盼望已久的“一（E，EtherNet）网到底”或“一（E，EtherNet）网打尽”的局面开始显现。为此，本章先对以太网的有关发展及其技术优势做介绍，接着介绍上述 3 种工业以太网。

本书对上述网络的介绍都是先简要介绍其组成、协议、机理、结构及特点，进而结合有关厂家的产品介绍一些典型的配置实例。对具体网络的叙述，本书则在一般概括与具体介绍两个方面做了努力。前者是为了能全面理解这些网络的结构与特点，把握 PLC 网络系统的全貌，便于通过对比组建网络。后者是为了能分类了解这些网络的应用与使用，弄清 PLC 网络组态的思路，便于按照步骤设置好网络。

相比已有介绍 PLC 网络的专著，像本书这样抓住 PLC 网络的当今主流，把握 PLC 网络的发展趋势，从网络机理到应用配置做系统说明，对各个品牌 PLC 网络做全面介绍，似乎还未曾有过。这里的主流、趋势、系统、全面也正是本书追求的目标。

但毕竟网络配置的细节很多，特别是网络具体产品的类型、型号、版本、规格及安装的细节很多，还有网络的测试及排故障的内容更多，由于本书篇幅有限，实难一一顾及。何况 PLC 网络还在发展，很多新技术也很难一一概括。加上本人水平、精力及条件所限，书中不足之处，以至于存在差错也在所难免。在此，望广大读者不吝赐教！本人将诚恳采纳大家的意见，向着本书追求的目标，把本书修改好，以使其成为您进行 PLC 网络系统配置的好向导。

本书涉及了各种 PLC 网络协议及各厂家的 PLC。使用术语相同，但含义可能不完全一样，还可能用不同的术语，但含义却是相同的。所以，建议读者阅读时多加留意，从实质上去理解就好处理了。

宋伯生　2010 年 12 月　于沈阳

目　　录

前言

绪论 …… 1

第 1 章　PLC 网络基础知识 …… 13

1.1　PLC 网络物理连接 …… 13

1.1.1　网络通信媒体 …… 13

1.1.2　网络通信组件 …… 19

1.1.3　网络拓扑结构 …… 21

1.2　PLC 网络通信技术 …… 24

1.2.1　通信方式 …… 24

1.2.2　通信数据 …… 27

1.2.3　数字传输 …… 30

1.2.4　模拟传输 …… 34

1.2.5　通道复用 …… 37

1.3　网络结构模型与相应协议 …… 39

1.3.1　OSI/RM 模型与相应协议 …… 40

1.3.2　TCP/IP 模型与相应协议 …… 45

1.3.3　企业网络模型 …… 47

1.4　计算机局部网络与 PLC 网络协议标准 …… 48

1.4.1　计算机局部网络标准 …… 48

1.4.2　PLC 网络行业标准 …… 57

1.4.3　PLC 网络事实标准 …… 61

1.5　PLC 网络及其配置 …… 65

1.5.1　PLC 网络概况 …… 65

1.5.2　PLC 网络特点 …… 76

1.5.3　PLC 网络配置 …… 78

1.6　PLC 网络通信实现 …… 80

1.6.1　自动通信 …… 80

1.6.2　对话通信 …… 83

1.6.3　专用软件通信 …… 84

1.6.4　互联网通信 …… 86

1.6.5　利用公网通信 …… 87

第 2 章　PLC 串口网络配置 …… 88

2.1　计算机标准串口 …… 88

2.1.1　RS-232C 接口 …… 88

2.1.2　RS-422A 接口 …… 92

2.1.3　RS-485 接口 …… 92

2.1.4　USB 口 …… 93

2.1.5　IEEE1394 口 …… 95

2.1.6　通信口转换 …… 95

2.1.7　串口设定 …… 97

2.2　LM 机串口网络 …… 97

2.2.1　LM 机串口配置 …… 97

2.2.2　LM 机串口功能 …… 99

2.2.3　LM 机串口设置 …… 99

2.2.4　LM 机串口连网配置实例 …… 99

2.3　OMRON PLC 串口网络 …… 100

2.3.1　OMRON PLC 串口配置 …… 100

2.3.2　OMRON PLC 串口功能 …… 105

2.3.3　OMRON PLC 串口设置 …… 108

2.3.4　OMRON PLC 串口连网实例 …… 111

2.4　西门子 PLC 串口网络 …… 115

2.4.1　西门子 PLC 串口配置 …… 115

2.4.2　西门子串口通信协议 …… 119

2.4.3　西门子 PLC 串口网络设定 …… 121

2.4.4　西门子 PLC 串口网络配置实例 …… 127

2.5　三菱 PLC 串口网络 …… 129

2.5.1　三菱 PLC 串口配置 …… 130

2.5.2　三菱 PLC 串口功能 …… 131

2.5.3　三菱 PLC 串口设定 …… 132

2.5.4　三菱 PLC 串口使用实例 …… 133

第 3 章　PLC 设备网及其配置 …… 136

3.1　PLC 设备网概述 …… 136

3.1.1　PLC 远程 I/O 网 …… 136

3.1.2　现场总线 …… 138

3.1.3　PLC 设备网 …… 141

3.2　AS-i …… 142

3.2.1　AS-i 简介 …… 142

3.2.2　西门子 PLC AS-i 网络组件 …… 149

3.2.3　西门子 PLC AS-i 网络配置实例 …… 156

3.2.4　三菱 PLC AS-i 网络及其配置实例 …… 159

3.3　CC-Link/LT ………………………… 168
3.3.1　CC-Link/LT 简介 …………………… 169
3.3.2　三菱 CC-Link/LT 组件 …………… 172
3.3.3　三菱 CC-Link/LT 配置过程及实例 ………………………………… 180
3.4　CompoNet …………………………… 185
3.4.1　CompoNet 简介 …………………… 185
3.4.2　OMRON CompoNet 组件 ………… 191
3.4.3　OMRON CompoNet 配置实例 …… 196
第 4 章　PLC 控制网配置 ………………… 201
4.1　PLC 控制网概述……………………… 201
4.1.1　专用 PLC 控制网 ………………… 201
4.1.2　基于标准的 PLC 控制网 ………… 203
4.2　CC-Link …………………………… 203
4.2.1　CC-Link 简介……………………… 204
4.2.2　三菱 CC-Link 组件 ……………… 215
4.2.3　三菱 CC-Link 配置实例 ………… 219
4.3　DeviceNet …………………………… 230
4.3.1　DeviceNet 简介 …………………… 230
4.3.2　AB DeviceNet 组件及配置实例 … 237
4.3.3　OMRON DeviceNet 组件及配置实例 ………………………………… 248
4.3.4　三菱 DeviceNet 组件及配置实例 ………………………………… 255
4.4　ControlNet ………………………… 256
4.4.1　ControlNet 简介 …………………… 256
4.4.2　AB ControlNet 组件及配置实例 … 264
4.4.3　OMRON Controller Link ………… 277
4.5　Profibus …………………………… 293
4.5.1　Profibus 简介 ……………………… 294
4.5.2　西门子 PLC Profibus 组件及配置实例 ………………………………… 298
4.5.3　和利时 PLC Profibus 组件及配置实例 ………………………………… 316
4.5.4　其他 PLC 公司 Profibus 组件 …… 320
第 5 章　PLC 信息网配置 ………………… 326
5.1　以太网发展 ………………………… 326
5.1.1　传统以太网 ……………………… 326
5.1.2　快速以太网 ……………………… 327
5.1.3　交换以太网 ……………………… 330
5.1.4　工业以太网 ……………………… 335
5.1.5　PLC 以太网 ……………………… 337
5.2　和利时 PLC 以太网配置 ………… 338
5.2.1　LM 机以太网模块特性 ………… 338
5.2.2　LM 机以太网模块功能 ………… 339
5.2.3　LM 机以太网设置 ……………… 340
5.2.4　LM 机以太网使用实例 ………… 342
5.3　AB PLC 以太网配置 ……………… 342
5.3.1　Ethernet/IP 简介 ………………… 343
5.3.2　AB 以太网组件 ………………… 345
5.3.3　AB 以太网配置实例 …………… 347
5.4　OMRON PLC 以太网配置 ……… 354
5.4.1　以太网组件 ……………………… 354
5.4.2　以太网功能 ……………………… 357
5.4.3　以太网设置 ……………………… 362
5.4.4　以太网配置实例 ………………… 368
5.5　西门子 PLC 以太网配置 ………… 371
5.5.1　Profinet 简介 ……………………… 371
5.5.2　西门子以太网组件 ……………… 378
5.5.3　西门子 PLC 以太网配置实例 …… 382
5.6　三菱 PLC 以太网配置 …………… 400
5.6.1　CC-Link/IE 简介 ………………… 400
5.6.2　三菱 CC-Link IE 组件及配置实例 ………………………………… 405
5.6.3　三菱信息网组件及其配置实例 … 410
参考文献 ………………………………… 414
后记 ……………………………………… 415

绪　　论

1. PLC 网络概念

PLC 网络是指分布在不同地理位置上、各自独立工作的 PLC、计算机或现场设备，通过通信组件与通信介质进行物理连接，并在网络软件及通信程序管理与协调下，实现数据通信、信息交流的集成系统。PLC 网络是计算机、PLC、现场设备及现代通信技术发展的产物，并随着这些技术的进步而日趋完善！与单一的 PLC 控制系统相比，它可实现更大规模、更广范围的实时控制，更全面、更精确的信息处理。同时，由于控制的网络化、分散化，控制出现故障的风险也将减少。

在 PLC 网络中，各个独立工作的 PLC、计算机或现场设备称为网络站点（node），简称站点或节点。

PLC 网络站点的多少，取决网络的规模。多的有几十，甚至更多。少的只有几个、十几个，甚至于仅两个。如仅拥有两个站点的网络有时也称链接。

PLC 网络还可互连。指的是，通过专用的网络互连组件或同时连接在不同网络上的站点，使不同网络相互连接，从而实现不同网络站点之间的通信。互连后的网络是网络的网络，称互连网（也称互联网，internet 或 inter network 或 interconnection network），其实质也是网络。

这里对 PLC 网络的界定强调了它是“集成系统”。也就是由一些单一的系统所集成。显然比前者要复杂得多。具体讲，构成 PLC 网络有 3 个要点：

（1）应有物理连接

目的是在站点间建立通信通道。为此要做到：

1）要选用好通信媒体或介质。通信介质可以是有线的，如电缆、光缆；也可以是无线的，如无线电波、光波、红外线。类型很多，到底选用什么介质，则与网络的站点最大距离、网络站点数目、分布情况以及工作要求及环境有关。

2）要选用好网络组件，主要是配置与使用好网络模块或相应接口。以便用它通过通信介质实现站点间的物理连接。

对计算机，如串口连网，可使用串口或 USB 口；如果接入其他类型的 PLC 网络，那就要插入相应的网卡。

对 PLC，如串口连网，可使用 CPU 单元上的外设口、串口或 USB 口，也可用串口模块；如果连接其他类型的网络，那就要配置相应的网络插件或模块。

对现场设备，如串口连网，可使用串口或 USB 口；如果要连接其他类型的网络，那就要配置相应的专用网络接口。

当网络站点之间的距离很大时，为确保数据正确传输，需增设相关通信组件，以进行信号放大或数据中转。而为了网络互连，则还要有相应的网络组件。

（2）应有数据通信

目的是进行站点间信息交流。

对于 PLC 网络，信息主要有两个方面：一是状态信息，它包含自身工作及控制对象工作的状况；二是命令信息，它包含通信命令发送、应答及工作命令下达。

状态信息交流可使各个 PLC 站点的控制得以协调，进而提高控制能力。同时，状态信息，特别是所收集的对象状态信息，还可上传，为企业的信息管理提供原始数据。

命令信息的传送及应答，是各站点相互操作的需要。这也是 PLC 网络所特有的。如 PLC 控制变频器的输出频率就可用传送命令信息实现。再如计算机控制 PLC 工作，或 PLC 主站控制其从站工作，用的也是命令信息。

数据通信进行信息交流要做到以下两点：

1）要有网络管理软件，以进行网络配置与管理。对 PLC 网络，PLC 厂家的编程软件多可进行这个配置与管理。如站点编址、通信参数设定、使用数据区指定等。此工作也称为网络组态或设置（定），是使用网络必须做好的工作。此外，有的厂家也还提供有专门网络管理软件，也可用以对网络的组态及管理。

2）要有通信程序，以进行通信数据的准备、传送、接收、处理及使用，进而达到交流信息、传送命令的目的。对 PLC 网络，这个程序必须由用户编写，要依据控制进程以及交流信息的需要编写。

（3）应有 PLC 站点

PLC 应该是网络的核心。

PLC 网络的数据通信主要是在 PLC 与计算机、PLC 与 PLC 以及 PLC 与现场设备间进行。在这 3 种通信中，唯一不能缺少的就是 PLC。显然，如果网络中没有 PLC，只有计算机，那只是计算机网络。如果连计算机都没有，那可能是电信或电视网络。

各站点都能独立工作也是必要的。计算机、PLC 独立工作比较好理解。而这里的现场设备则强调要有智能，即不仅要有通信接口，还要有简单的控制功能。否则，只是 PLC 的远程 I/O 系统，与计算机与打印机之类的设备连网一样，虽也是网络，但从控制风险分散的角度看，似乎不是真正意义上的网络。真正意义上的网络，应保证即使网络数据通信瘫痪，但由于各站点都能独立工作，都可实施自身简单的控制，还可确保系统工作的安全。

总之，物理连接、数据通信及有独立工作的 PLC 站点是 PLC 网络的 3 个要点。缺少其中一个都不能称为 PLC 网络。

2. PLC 网络类型

PLC 网络的类型是很多的，可以说是一个 PLC 公司一个样。而且相互多不兼容。有的即使是同一公司的网络，但网络类型不同，PLC 机型不同，网络也不完全相同，也不兼容。这也是 PLC 网络的悲哀！当然，事情也在变化。由于 PLC 网络标准化的推进，各 PLC 厂家的网络，已逐渐向若干公认的标准靠近。有的厂家还生产有可接入这些公认网络的模块。有了它，也可使自身的 PLC 接入这些公认网络。

尽管 PLC 网络千差万别，但还是可从实现功能及站点角色上对其作分类说明。

（1）从网络功能角度分类

1）设备网（Field），也称现场网络，有的称现场通信网或现场总线（有的也把一些控制网归类到现场总线中）。主要用于 PLC 与现场设备及传感器/执行器之间的通信，以实现 PLC 对现场设备及智能装置的数据采集与工作控制。有了设备网，可以减少硬接线，减少安装时间及安装费用。同时，还便于实施对现场及现场设备实时诊断。

设备网处于企业网络的下层，交换数据量小。但通信的可靠性、实时性要求高。即使短时间的数据交换停止，将影响 PLC 控制功能的实现。

2）控制网（Control），相当于车间级或生产线级的网络，有的称为数据及现场通信网，主要用于 PLC 间的连网、通信，以实现 PLC 对多台设备或生产线控制的协调，以扩大 PLC 的控制范围，增强 PLC 的控制能力。

控制网处于企业网络的中层。它交换数据量也不大，但通信的可靠性、实时性要求也很高。一般讲，即使短时间的数据交换停止也是不允许的。

3）信息网（Information），也就是企业级网络，有的称为数据通信网，主要用于 PLC 与计算机连网通信。以使 PLC 与计算机或计算机与计算机交换信息、传达命令，以实现企业的供、产、销的信息共享，及人、财、物的资源管理。在此，PLC 起到对生产一线的数据采集、上传，管理命令下达等不可代替的作用。

信息网也是企业的局域网，是小范围的网络，覆盖范围可在十几千米以内，结构简单，布线容易。但它处于企业网络的上层，其通信的数据量大，要求通信的速度高。但通信的实时性要求可低些。即使较长时间停止数据交换也是允许的。

这 3 层网络还可互连。其办法是有的站点有两个通信接口。分别与不同层的网络相连。由于有这样网络互连，可很容易把工厂底层的信息上传到信息层；或把信息层的命令下达到现场。

要指出的是，这样划分也是相对与变化发展的。如控制网，虽主要用在 PLC 之间的通信、交换数据，但也可在计算机与 PLC 以及 I/O 设备与 PLC 之间通信、交换数据。再如信息网，情况也类似。特别是随着以太网技术的应用以及以太网技术的进步，除了以太网自身的网速高、组网简单、成本低廉、软件丰富、互连容易、使用方便、应用广泛这些固有的优点外，它在工业应用中的环境适应性、组装方便性、工作可靠性、信息安全性以及通信实时性也都有很大长进。因而已出现“e 网包打天下”的局面。极有这样可能，在未来 PLC 的 3 种网络中，都使用以太网。果真那样，也许 PLC 的组网将会变得更简单、更方便与更低廉，其应用也更广泛、更普及与更有效。那将是控制自动化、信息化、网络化发展的幸事！

（2）从站点角色分工分类

1）主从网（Master/Slave，M/S）。在这样网络中，多数站点为从站，只有一个或个别几个站为主站。主站管理从站，并发起通信。而从站则接受管理，响应通信。PLC 网络大多数为此类网络。如 Profibus-DP 网，就有主站、从站之分。

主、从网较复杂，在组网时，要进行相应组态或设定。但是它较易实现集中管理与监控，安全性高，较适合作为控制网与设备网。

2）客户机、服务器网（Cline/Server，C/S）。在这种网络中，多数站点为客户机（Client），只有一个或个别几个站为服务器。

计算机网络很多是这样系统。这里的服务器（Server）一般为高性能的计算机。客户机一般是指普通计算机，也可称网络工作站。服务器运行网络操作系统，进行网络管理，提供共享资源。处理各个网络工作站的服务请求。如访问服务器硬盘上的文件系统、申请共享打印服务等。客户机，也即网络工作站，是用户使用网络的接口，也是用户工作的平台。它接受网络服务器管理与服务，共享网络的资源。

PLC 网络的 C/S 系统，服务器则多为 PLC，用以采集数据，而计算机则可能是工作站，

用以访问 PLC，读取数据。将要介绍的 SCADA 系统就是这么处理的。

3）网站（网页）、浏览器网（Brower/Server，B/S）。将要提到的因特网就是这样的网络。在这种网络上，有无限多的站点。但这些站点大致可分为两类：一类是提供服务的，另一类是接受服务的。前者设有网址，以网页的形式提供数据、画面或多媒体数据，供后者访问。后者使用通用的浏览器，通过登录访问前者，接收前者服务。

PLC 网络的 B/S 系统，服务器也多为 PLC。这时，PLC 要有可以提供生成网页的以太网模块。用它可建立 PLC 实时数据网页，以让计算机通过浏览器访问。这比用 SCADA 更为简便，成本也较低。只是由于 B/S 产品人机交互界面比较差，远程打印瓶颈问题，还有报表设计问题，安全问题、接入速度问题等等，制约了 B/S 产品的普及。

4）对等网。在这种网络中，各个站点不分主次。每个站点都可以对等地与其他站点通信。此类网络比较简单，组网方式灵活方便。著名的以太网就是对等网。PLC 串口自由协议通信，通信双方也是对等的。

在对等网中，各方都可共享彼此的信息资源和硬件资源。但是它较难实现集中管理与监控，安全性也低。

5）链接网。使用各个站点间指定数据区共享、运用数据链接自动通信。在通信时，各个站点也是对等的。但与对等网不同的是，它要通过网络设定，指定有一个管理主站，以实施对网络管理。

（3）从网络覆盖范围分类

如仅考虑计算机站点构成的网络，其覆盖范围相差很大，类型很多。最小的是个人网络，仅供一个人使用。例如，通过无线网络，将一台计算机与它的鼠标、键盘和打印机连接起来，就是这样的网络。最大的可以覆盖整个地球，可供全球人员使用。例如因特网。表 0-1 所示为站点之间距离、所处位置及网络例子。但是，PLC 网络覆盖范围变化不大。

表 0-1　计算机网络的不同覆盖范围

站点之间的距离	站点所在的位置	例　子
1m	1m 见方的范围内	个人区域网
10m	同一房间	局域网
100m	同一建筑物内	
1km	同一校园	
10km	同一城市	城域网
100km	同一国家	广域网
1000km	同一个洲	
10000km	同一个行星	Internet

1）广域网（Wide Area Network）。可覆盖一个省、几个省、一个国家或几个国家的计算机网络。PLC 无此网络，但可接入此网络。

2）城域网（Metropolitan Area Network）。可覆盖一个城市的计算机网络。目前，我国许多城市已建立或正在建立这样的网络。PLC 多无此网络，但也可接入此网络。如特殊情况需要，也可建立此网络。例如，笔者曾参与编程的，山东威海市自来水公司组建的调度中心计算机，通过串口无线 Modem 与多个水站的西门子 S7-200PLC（其串口也连接无线Modem），

通过无线信道连网就是一例。该网覆盖的地域就是整个威海市，也是典型的城域网。

以上两个网络可以是公用的，公众付费即可使用这个网络。也可是专用的，如金融网络，虽也是城域网、广域网，但并不是任何计算机用户都可以接入。

显然，如果采集现场数据的 PLC 与读取 PLC 所采集的数据计算机都接入此公用网，也就可实现计算机对 PLC 数据的远程读取，实际也就是 PLC 的广域网或城域网。

3）局域网（Local Area Network）。覆盖地域不大的网络。以上介绍的企业信息网即为此网络。PLC 常要接入此网络。

4）因特网（Internet，这里字母 i 是大写!）。是互联网（internet）的一种，指世界范围互联网，也是最大的广域网。其前身是 1969 年诞生在美国的阿帕网（ARPANET）。它用 TCP/IP 网络协议将各种不同类型、不同规模、位于不同地理位置的计算机网络连接成一个整体，提供有万维网、文件传输、电子邮件、远程登录等服务。而万维网则是它的最重要的应用。PLC 也常要接入此网络。

这里的所谓万维网，是指环球信息网（World Wide Web，WWW），简称 3W，有时也叫 Web，是欧洲粒子物理实验室（CERN）于 1989 年研制的。它创建了超文本（hypertext）标记语言（HTML），使用“超级链接”，把因特网上的所有信息，如图像、动画、声音、3D 世界等，连接在一起，形成巨大的分布资源，使得任何连接因特网的用户都可通过 Web 浏览器，访问这些资源，共享这些信息。

文件传输、电子邮件是人们上网很常见的使用。至于远程登录，是指通过因特网，允许一个用户登录到一个远程计算机系统中，就好像用户端直接与远程计算机相连一样。一般人使用不多。

提示：习惯上往往把因特网、万维网统称为互联网。

5）接入网（Access Network）。是指计算机或局域网到因特网之间的中介。一般由因特网服务商（ISP）提供。ISP 提供的接入网有 3 种：

① 电话网络接入。低速的可以用调制解调器（Modem）拨号入网；高速的可用 ADSL 宽带入网。

② 有线电视网络（混合光纤电缆系统，HFC）接入。用 Cable Modem 入网。由于有线电视的普及，这种接入目前已用得很多。

③ 移动网络。计算机使用无线网卡，通过 ISP 供应商提供的账号接入因特网。这为笔记本计算机用户提供了很大方便。只是这样的 ISP 是很多的。也是多层次的。最高层次的 ISP 才拥有专用通信通道直接接入因特网。

当配置以太网模块或接口的 PLC 接入因特网后，也可设置网址，供用户远程访问。有的还可制成网页，用户利用浏览器即可直接读取 PLC 的数据。这样，就可以使 PLC 控制的状态信息传递到世界的任何可接入因特网的地方。也可从世界任何可接入因特网的地方得到 PLC 所需要的命令信息。PLC 控制再也不是信息的孤岛了。这对实现控制信息化、网络化、远程化，提高 PLC 控制效益提供了很大的方便。

（4）从网络传输介质分类

1）有线网络。网络站点之间的物理连接均使用电缆或光缆这样的有线传输介质，是最常见的，也是最常用的 PLC 网络。

2）无线网络。网络站点之间的物理连接不完全使用有线传输介质，还使用电磁波、光

波、红外线这样的传输介质。

计算机的无线网络类型很多。小的如系统无线连网，它用蓝牙技术实现计算机组件之间的连接，如键盘、鼠标与主板连接。大的有无线局域网（WLAN），这种网络的每个站点都用一个无线调制解调器及通信天线做物理连接，进而实现相互通信。更大的也可使用基于基站（基站间用有线通信）的移动通信以组成广域网，这是因为移动通信早已从模拟通信发展为数字通信，所以它除了传送话音，也可用于数据交换。此外，还可利用无线路由器，或移动网络接入因特网，其通信范围将不受限制。

无线网络接线简单，站点还可移动，网络站点接入、退出灵活，为它的广泛使用提供了很大方便，目前在 PLC 网络中也已用得越来越多。

3. PLC 网络功能

PLC 网络功能是实现 PLC 与 PLC、计算机（还有人机界面）及现场设备之间通信。而通信则各有其目的。

（1）PLC 与计算机、人机界面通信的目的

1）实现 PLC 编程及程序调试。这也是 PLC 与计算机通信的最基本目的。PLC 编程是较麻烦的。若用手持编程器，通过助记符编程则更麻烦。但若用计算机与 PLC 连网，再使用相应编程软件，则可使用梯形图或流程图语言编程，甚至于还可用其他高级语言编程，较为方便。

而且用计算机编程，还可对所编的程序进行语法检查，以便于发现与查找程序中的语法错误。同时，还可进行程序仿真，可对输入点的状态进行强制置位或复位，可模拟现场情况，进而可发现与解决程序中语义方面的问题。

此外，计算机编程还可存储、打印 PLC 程序，或把程序写入 ROM 中等，便于 PLC 程序的移植及重用。

所以与计算机连网进行 PLC 编程已是一个趋势。有的厂家高级的 PLC 编程器，实质就是笔记本式个人计算机。

2）实现计算机控制系统的监控与数据采集 SCADA（Supervisory Control and Data Acquisition）。具体是：

① 读取 PLC 工作状态及 PLC 所控制的 I/O 点及内部数据的状态，并显示在计算机的屏幕上，以便于人们了解 PLC 及所控制设备的工作状态。

② 通过向 PLC 写数据，改变 PLC 所控制的设备工作状况，或改变 PLC 的工作模式，实现人们对控制的必要干预。

③读取由 PLC 所采集的数据，并进行处理、存储、显示及打印，便于人们使用。

3）实现人机界面的监控及管理。人机界面（HumanMachineInterface）实质是工业现场用的简易计算机。具有信息处理、数据录入、采集及显示功能。近来已用得越来越多。

它与 PLC 连网通信，可从 PLC 读取数据，并予以显示。也可向它写数据，再传输给 PLC，改变 PLC 的状态或数据，实现对 PLC 或系统的控制。

虽然它的功能不如计算机，但它的体积小、工作可靠，可安装在工业现场。所以用起来是很方便的。在一定程度上也可起到计算机的 SCADA 作用。

4）实现远程诊断与维护。有的 PLC 配备有远程诊断与维护系统。可通过连网，甚至互连网，利用厂家提供的通信模块与专用软件，实施远程数据采集与故障诊断，并实施相应维

护，如下载新版本的 CPU 操作系统及有关硬件驱动等。

（2）PLC 与 PLC 的通信目的

1）扩大控制地域及增大控制规模。PLC 多安装于工业现场，用于当地控制。但如果进行连网通信，则可实现远程控制。距离近的可以为几十、几百米，远的可达几千米或更远，可大大扩大 PLC 的控制地域。

连网后还可增加 PLC 控制的 I/O 点数。这里，尽管每台 PLC 控制的 I/O 点数不变（有的 PLC 加远程单元后，也可增加 I/O 点数），但由于连网后，为多台 PLC 参与控制。其控制总点数为参与连网的 PLC 控制点数之和。显然，其控制的规模要比单个 PLC 的规模大。

不少事实说明，两个或若干个中、小型 PLC 连网，也可达到一个大型机的控制规模，而费用则比大型机要低得多。因而用中、小型 PLC 连网，去替代大型 PLC，已成为一个趋势。

2）实现系统的综合及协调控制。用 PLC 实现对单个设备的控制是很方便的。但如果有若干个设备要协调工作，用 PLC 控制，较好的办法是连网通信。单个设备各由各的 PLC 控制，而设备间的工作协调，则依靠连网通信后 PLC 间的数据交换解决。

这样连网通信，可使 PLC 控制，从设备一级提升到对生产线一级。便于实现工厂的综合自动化。

3）提高 PLC 工作的可靠性。连网通信后各 PLC 还是独立工作的。只要协调好，即使个别站点出现故障，并不影响其他站工作，更不至于全局瘫痪。故可降低系统的故障风险。

4）连网通信更便于实现冗余配置。工作 PLC 与热备用 PLC 使用连网通信处理转换，用起来非常方便，系统也非常可靠。是当今冗余配置的一个趋势。

（3）PLC 与现场设备通信目的

1）简化系统布线。工业现场的普通开关量及模拟量输入、输出信号，都是通过信号线与 PLC 的 I/O 点相连。连线很多，布线也很复杂。特别是一些远离 PLC 的输入、输出点多时，则更为复杂。而如果用连网通信传送输入、输出信号，则简单得多。因为通信线仅用两根或几根，就可传送很多输入、输出信号。尽管这样处理有一定延时，但由于网络传送及信号处理速度的不断提高，这点时延，对一般的控制过程是不会有什么影响的。

2）便于系统维修。输入、输出信号用连网通信处理，布线简单了。这既可节省硬件开销，还便于系统维修。可以设想，在一大堆的输入、输出接线中，真有个别出现问题，在现场查找是很不易的。

3）实施对现场设备的管理。目前很多现场设备都有自身的 CPU、内存及通信接口。自身可采集、处理或使用数据。但是，如果没有连网通信，它们还只是“信息孤岛”。无法与其他控制协调，或实现信息共享。而如果与 PLC 连网通信，则将可使这些装置不再是“信息孤岛”了。

特别要强调的是，信息化已是当今信息社会的潮流。已给世界带来了巨大的社会效益与经济效益。而企业的信息化，推行企业资源计划（ERP）、信息执行系统（MES），甚至于产品生命周期计划（PLM），更是给企业带来了不可估量的效益。

而企业信息化的基础是准确的生产一线数据。PLC 连网通信后，这些数据可自动采集，

避免了人为干扰，因而是客观的、准确的，而且是完整的、及时的。这就为建立智能工厂、透明工厂、全集成系统或 e 自动化等的成功提供了基础。

总之，从根本上讲，PLC 连网通信主要是用好信息技术。目的是协调控制，进而实现系统控制的自动化、网络化、远程化、信息化、智能化。

4. PLC 网络性能

PLC 网络是用于站点间数据通信的。为此，要求这个通信做到速度快、实时性好、可靠性高、出错率低、传输数据量大。同时，网络还要便于使用、维护。而且建网及使用的费用要低廉。为了反映网络的这些特性，可以使用一些指标予以衡量。这些指标也是人们对 PLC 网络的配置与使用的要求。这些指标主要是：

（1）网络规模

指的是网络可连接的最多站点数。PLC 网络站点少的仅 2、3 个，多的有 8、16、32、64、128 个不等。功能强的网络，最多站点数也将多些。

网络规模还要看网络互连的情况。网络互连得多，网络规模也大。

（2）网络覆盖

指网络中站点间最大的距离。PLC 网络最大站点间距离差别很大。小的几米、十几米，甚至也可能同在一个电气柜内。大的可以是几百米、几千米，甚至几十千米。功能强的通信媒体使用光纤的站点间的距离则大些。

PLC 网络规模及覆盖比起计算机网络要小得多。不大可能有什么城域网、广域网。即使企业级的 PLC 网络，主要也是用以实现 PLC 与计算机信息交流。纯 PLC 站点的网络最多也只是车间级的。

（3）帧的大小

帧是网络数据传送的单位。一般以二进制位或一个字符计。这里“帧的大小”是指，一个帧的最大二进制位数或字符数（两者都是以字节计）。这个指标与网络的性能有关。性能强的网络，帧的最大字节数多，如几 K 字节。性能差的网络，有的只有几十字节或 100 多个字节。

由于帧的大小是受限制的。所以如果一次要传送的数据（即报文），很大，一般要把它分解成若干个帧，按帧分别传送。

（4）网络速度

指网络数据信号发送或接收的速率。常用的有两个指标：一是比特率，又称为信息速率，简称数据率。比特是二进制数的一个位。比特率 S 是指每秒平均传输比特的个数，其单位是每秒位（bit/s），或每秒千位（kbit/s），或每秒兆位（Mbit/s）。

二是信号码元（信号波形）传输速率，即波特率。指每秒可传送的波形数量。信号波形是承载信息的基本信号单位，也是信号编码的单位。波特率 B 与波形持续的周期 T 有关。两者互为倒数。

比特率和波特率及其携带的信息量有关。其关系可以按下式计算：

$$S = B\log_2 n$$

这里，n 代表信号波形中包含的信息量，即波形可反映多少数值有关。如为 2，即仅反映 0、1 两种状态，则 S 与 B 完全相等。如为 4，可反映 00、01、10、11 等 4 种状态，则 $S = 2B$。多数 PLC 网络信号波形的信息量为 2，所以，波特率与比特率总是相等的。

波特率也可比比特率大。如 10M 以太网，其比特率为数据率为 10Mbit/s。但它使用曼彻斯特编码。这意味着发送的每一位要有两个信号周期。所以，其码元传输速率即为波特率，是数据率的两倍，即 20M 波特。

网络速率有时也用带宽（bandwidth）表示。带宽本是模拟信号通信线路传输能力的术语，指传输信号所包含成分的频率范围。如电话线路，可传输话音信号，其范围为 3.1Hz（从 3.1～3.4Hz）。当今，也用它近似代表通道传输数字信号的最高速率。因为带宽的下限是很小的。带宽的单位与比特率相同。

（5）通信时延（delay 或 latency）

通信时延指一个帧的数据从网络的一个站点传输到另一个站点所需的时间。由发送时延、传输时延及处理时延三部分组成。

发送时延指发送站点把一个帧数据发送进入传输媒体所需要的时间。它与帧大小及信号发送速率（transmission 或 transmit）有关。即

$$\text{发送时延}=\frac{\text{帧大小}}{\text{信号发送速率}}$$

传输时延指信号在介质上的传输时延，与信号在传输介质上的传输速率（propagation 或 propagate）及信道长度有关。即

$$\text{传输时延}=\frac{\text{信道长度}}{\text{信号传输速率}}$$

信号传输速率与介质的特性有关。如在粗同轴电缆上传播，约为 200m/μs（相当于光在真空中传播速度的 2/3）。

处理时延指通信站点或网络组件处理通信数据所需的时间。与站点或组件特性及数据的多少有关。但不大好量化计算。

PLC 网络时延不能太长。特别是它的设备网与控制网，只能以 ms（毫秒）计，否则将影响控制的及时性。进而也将影响控制精确度。

还有一个指标叫抖动，指数据报（帧）之间延时差异。当然这个值应尽可能小为好。

（6）通信质量

通信质量一般用差错率，也即误码率衡量。其值为

误码率(Pe)＝(接收方出现差错的码元数(位数)/总的传输码元数(位数))×100%。

误码率是一个统计平均值，在统计和测试时应采用统计学的方法，在足够时间和足够统计的数量后方可正确得出。

计算机网络通信系统中，要求误码率低于 10^{-6}。如果实际传输的不是二进制信号，需折合成二进制信号计算。PLC 控制与设备网络要求误码率更小。一般讲，任何出现误码都是不允许的。或一旦出现误码，也要有相应的应对措施。

（7）网络可靠性

可用可靠度衡量。即

$$\text{可靠度}=\frac{\text{全年(或全月)正常工作时间}}{\text{全年(或全月)总工作时间}}\times 100\%$$

影响可靠度的因素很多，主要是网络的软、硬件可靠性及操作人员的水平。

PLC 网络的可靠性还可用 RAS，即 Reliability（可靠性）、Availability（有效性）、Serviceability（可维护性）衡量，并设定有响应的评价指标。

（8）通信安全

主要指数据的安全。要有必要的措施，确保数据不能被无关人员盗用，也不能让黑客入侵。

（9）网络兼容

网络兼容也是必要的。目前，PLC 网络的兼容性很差。随着技术的发展及协调，这个不兼容的局面必然会有所改变的。

（10）网络经济性

指组建网络与使用、维修网络的费用。在其他性能相同或相近似，应选择此费用尽可能低的解决方案。

网络经济性还有一个指标是带宽的利用率。带宽是指在一个信道上用于传输信息的可用频率范围。它是用来表示信道传输能力的指标。因此带宽越宽，电路能够传输的信息量就越大。带宽的单位一般用频率使用的单位，即 Hz 或 MHz；也可用传输速率的单位比特率，即 bit/s；如果频率很高，如传输媒体用光纤，也有用波长（光速/频率），即 km 来表示的。

可以用带宽利用率衡量。利用率可用下式计算：

$$\eta = \frac{R_b}{B}$$

式中　R_b——比特率（bit/s）；

　　B——信道的带宽。

η 值大，说明带宽得到充分的利用。因而，也可获得更大的经济效益。

5. PLC 网络发展

如果说计算机网络是计算机技术进步与通信技术发展相结合的成果。那么，PLC 网络则是随着 PLC 技术的进步及计算机网络的发展而快速发展与逐步成熟起来的。

最初，与计算机一样，PLC 也没有网络。只有外设接口连接手持编程器，以编写、调试 PLC 程序，以及进行人机交互。

进一步发展，出现了图形编程器，显示屏尺寸加大，可用梯形图符号进行 PLC 编程。有的 PLC 的图形编程器实质就是当今的笔记本电脑。因而运用它，实际上就是计算机与 PLC 的链接。也许这就是 PLC 最初形态 PLC 与计算机连网。

再进一步发展是由于个人电脑价格大幅度降低及广泛应用，致使 PLC 编程几乎都是使用个人电脑加 PLC 编程软件。也就是说，PLC 与计算机的链接是很平常的事。

为了实现远程控制。PLC 还发展有远程单元。有远程主单元及远程从单元。主单元放置在当地的机架上，接受 PLC CPU 的管理。从单元放置在远程机架上，管理远程的 I/O 模块。

主、从单元通过通信介质实现物理相连，并进行通信，周期地交换远程 I/O 数据。把 CPU 对输出（O）的控制传送给远程输出模块，同时，把远程的输入模块的输入（I）传送给 CPU。这样，PLC CPU 处理远程 I/O 与处理当地 I/O 相比，所不同的只是时间略有延时（增加主、从模块间的通信时间）。

这样的远程控制，可扩大 PLC 的控制地域范围，还简化了 I/O 点的接线。对提供 PLC 的控制效能提到了重要作用。因此，这样的 PLC 远程控制，在 PLC 系统中至今仍然还在广泛应用。只是，这样的远程的控制系统，它的远程从站没有 CPU，不能独立工作，不是独

立站点。控制的风险要大些。而且严格说它只是分布控制系统，还不能算是网络。

这样远程系统的进一步发展，还出现了在从站中，也可接入小型 PLC 的情况。这也就出现 PLC 主、从控制网了。

以上可以说是 20 世纪 80 年代末期的情况。之后，各个 PLC 厂家都加快了 PLC 网络的开发，出现各种不同的 PLC 网络。

OMRON 有 Host Link 网（用于计算机与 PLC 通信）、PLC Link 网（用于 PLC 与 PLC 通信）、SYSMAC Link 网（用于 PLC 与计算机以及 PLC 通信）、SYSMAC NET 网（用于 PLC 与计算机以及 PLC 通信）、ComBoBus/S 及 ComBoBus/D 网（用于 PLC 与现场设备以及 PLC 通信）、ControlLink 网（用于 PLC 与计算机以及 PLC 通信）、以太网（用于 PLC 与计算机以及 PLC 通信）等。

西门子 S5 系列机网络且不论，S7 机除了可用 RS-485 串口建立 PPI 网、MPI 网进行一对一，或一对多的主从网络，还有 AS-i 网（用于设备层）、Profibus 网（用于控制层）、工业以太网（用于信息层）。

三菱 PLC 可用标准通信串口 RS-232C 口或 RS-485 口，进行 1∶1 或 1∶N 通信。此外还有 CC-Link 网、CC-Link/LT 网、MELSECNET/10、MELSECNET（Ⅱ）、MELSECNET/B、MELSECNET/H、MELSECI/O-LINK、MELSECNETFX-PN 及以太网。

Allen-Bradley、GE 及施耐德等公司的 PLC 网络也很多。

可以说，20 世纪 90 年代，是 PLC 网络百花齐放，越来越多的年代。

进入 21 世纪，情况则有所变化。出现了 4 个特点：

1. PLC 网络兼容在进步

经过实际使用比较及商业竞争、优胜劣汰，加上 PLC 标准化的推进，在 PLC 网络中，性能低的、兼容性差的逐步被淘汰了。各厂家的网络开始趋同或出现兼容。特别是新推出的 PLC，网络类型都向主流网络靠近，以致与旧机型的网络都不兼容了。

以信息网为例，当今各 PLC 厂家都是使用工业以太网。先是用 10M 以太网，继而用 100M 以太网、1000M 以太网，甚至速度更快的以太网也都在研发中。尽管各家以太网的具体细节不完全相同，但物理连接上各家基本都是相同的。此外，也出现了几个公认的上层协议。

再以设备网及个别控制网为例，当今各个厂家 PLC 都向现场总线靠近。公认有 Profibus-DP、DeviceNet 及 CC-Link。几乎各个厂家新型的 PLC 都提供接入这些网络的接口。

只是多数厂家的控制网差别大些，不大好兼容。但有厂家也提供有可接入两种不同网络的接口产品。有的类似网关，一边接入一家网络，利用它的收、发转换，间接实现了不同控制网的互连；还有的类似接口转换器，可在不同的网络间进行转换。也许这将是 PLC 网络发展的亮点。

2. PLC 网络功能在加多

以常用的标准串口连网为例。早期 OMRON PLC 只能作为从站，被动地与计算机通信；后来由于开发了串口指令，不仅可主动发起与计算机通信，而且还可与其他 PLC 或现场设备通信；同时还可实现多台 PLC 间的链接通信，也具有原先 PLC Link 网的功能。西门子的 S7-200 机用 RS-485 口多站点连网，早期只能是一个主站，而今也可配置为多个主站。再如以太网，近期的不仅速度快了，功能也有所加多。有的还可实现网页的功能等。

3. PLC 网络性能在提高

随着 PLC 自身技术的发展及通信技术进步，PLC 网络的规模、速度、可靠性也在提高。网络冗余也用得越来越多。

4. PLC 网络的应用增加

例如在现今 PLC 的应用中，一台 PLC 加一台简易人机界面是很平常的。这也是最简单的 PLC 网络。这样配置，虽会增加人机界面的费用，但可利用人机界面的画面实现按钮、指示灯的功能，得到输入、输出点减少及电气控制柜的简化。从而也可能出现增加人机界面，但费用可不增加或增加不多的情况。这也许是 PLC 加人机界面配置用得越多的原因吧！

更值得注意的是，由于 PLC 网络应用的发展，已出现了基于网络的控制系统。不仅数据采集、控制信号传输通过网络，而且控制算法的生成与执行也分散到各个站点。这样，不仅控制的内涵从基于信号（Signal）变换的顺序、过程、运动控制，提升到了基于信息（Information）处理的生产调度、经营管理的控制，进而实现控制的自动化、远程化、信息化及智能化。这样不仅可获得更大的效益，而且由于数据采集及控制的分散，既可分散风险，又可作冗余配置，将极大地提高系统的可靠性。

总之，PLC 网络除了自身的技术进步，还正在向着兼容、增强、提高及增加应用的方向发展。PLC 控制系统再也不会成为控制信息的“孤岛”了。原来通信能力较差的 PLC，目前已经走到了工业自动控制网络化的前列。

第 1 章　PLC 网络基础知识

在 PLC 网络中，尽管 PLC 是主体，但从技术的基本点上讲，PLC 网络与计算机网络是完全相同的。所以本章介绍的 PLC 网络基础知识当然包含计算机网络的知识。这些知识也是正确配置 PLC 网络所必需的。

1.1　PLC 网络物理连接

关键词：网络通信媒体、数据通信通道、无线通信介质、有线通信介质、网络通信组件、网络拓扑结构、星形结构、总线结构、环形结构、网状结构

网络物理连接是指怎样选用通信媒体、网络组件及拓扑结构，建立站点之间的通信通道，为实现网络通信提供硬件条件。主要的是要处理好 3 个问题：通信媒体的选择、通信组件的配置及选定站点连接的拓扑结构。

1.1.1　网络通信媒体

通信媒体也称通信介质，是网络站点间连接及传递信号的介质，是网络的基本构件。在 PLC 网络中，使用有多种介质。

通信信号在通信介质上传输，一般都存在两个问题。一是信号在传输过程中衰减，二是信号在传输过程中受干扰。衰减将使得接收端得到的信号太弱，以至于无法识别。同时从傅里叶分析可知，任何波形的周期信号总是由不同阶次的谐波组成，而信号传送速率高时，高阶次谐波的衰减是很快的。加上受介质分布参数的影响，不同阶次谐波的传输滞后又不同，所以即使信号不受干扰，传输后合成的波形也会有所失真。而如果传输过程还受有干扰，则将加重信号失真。信号失真则可能造成接收端即使收到了信号，也无法正确识别。

出现这两个问题都与网络传输信号的速率、距离，以及选用什么通信媒体有关。所以了解各种通信媒体特性，并依据网络传输信号的速率、距离，去合理选用媒体，是配置 PLC 网络的重要工作之一。

在 PLC 网络中，通信媒体分有线的与无线两大类。有线的有电缆与光缆。电缆，如铜、铝等金属导体，通过电流实现信号传输。光缆，是透明玻璃或塑胶绳，通过光波实现信号传输。无线媒体，通过电波、光波在自由空间传播进行信号传输。以下分别对电缆、光缆及无线介质进行介绍。

1. 电缆

有双绞线及同轴电缆。

（1）双绞线

双绞线（TwistedPair，TP）是两根绝缘导线按一定规则相互缠绕而成。通常将一对或多对放在一个绝缘套管中，并在其外面包上护套，以成为双绞线电缆，如图 1-1 所示。

双绞线通常用于传输平衡信号。也就是说，每条导线都带有电流，但相位相差 180°。

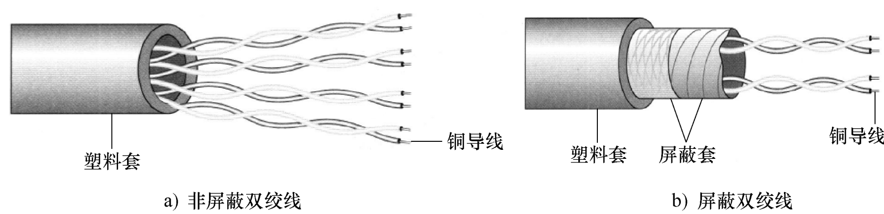


图 1-1　双绞线

外界电磁干扰给两个电流带来的影响将相互抵消，从而可减缓信号衰减。单位长度螺旋的数目越多，减缓的效果也越好。

双绞线按其是否有屏蔽，可分为非屏蔽双绞线（UnshieldedTwisted-Pair，UTP，见图 1-1a）和屏蔽双绞线（ShieldedTwisted-Pair，STP，见图 1-1b）。

屏蔽双绞线是在一对双绞线外面有金属筒缠绕，有的还在几对双绞线的外层用铜编织网包上，以用作屏蔽。此外，还在最外层，再包上一层具有保护性的聚乙烯塑料。屏蔽双绞线可降低外界的电磁干扰。然而，如果屏蔽层不连续或者屏蔽层电流不对称，反而会降低甚至完全失去屏蔽效果。STP 一般用在易于受电磁干扰和无线频率干扰的环境中。

无屏蔽双绞线除少了屏蔽层外，其余均与屏蔽双绞线相同。抗干扰能力较差，但它无屏蔽外套，直径小，可节省所占用的空间；重量轻、易弯曲、易安装；价格也便宜。所以，它已是目前 PLC 网络中使用频率最高的一种网线。

国际电工委员会和国际电信委员会 EIA/TIA（Electronic Industry Association/Telecommunication Industry Association）已经建立了 UTP 网线的国际标准并根据使用的领域分为多个类别（Categories 或者简称 CAT），这些类别线缆标准为

- Cat1：适用于电话和低速数据通信；
- Cat2：适用于 ISDN 及 T1/E1，支持高达 16MHz 的数据通信；
- Cat3：适用于 10Base-T 或 100Mbit/s 的 100Base-T4，支持高达 20MHz 的数据通信；
- Cat5：适用于 100Mbit/s 的 100Base-TX 和 100Base-T4，支持高达 100MHz 的数据通信。
- Cat5e：既适用于 100Mbit/s 的 100Base-TX、100Base-T4，支持高达 100MHz 的数据通信；又适用于 1000Mbit/s 的 1000Base-TX，支持高达 1000MHz 的数据通信。
- Cat6：适用于 1000Mbit/s 的 1000Base-TX，支持高达 1000MHz 的数据通信。

双绞线电缆中的每一根绝缘导线都用不同颜色加以区分，因此，很容易识别。每对有两根导线。其中一根导线的颜色为对应线的颜色，再加一个白色条纹。表 1-1 所示为 4 对非屏蔽双绞线电缆的电线颜色编码。

表 1-1　4 对非屏蔽双绞线电缆的电线颜色编码

线　对	颜色编码	简　写	线　对	颜色编码	简　写
线对 1	白-蓝	W-BL	线对 3	白-绿	W-G
	蓝	BL		绿	G
线对 2	白-橙	W-O	线对 4	白-棕	W-BR
	橙	O		棕	BR

（2）同轴电缆（Coaxial Cable）

同轴电缆是指有两个同心导体，而导体和屏蔽层又共用同一轴心的电缆。如图 1-2 所示，它由 4 个部分构成。1 是里层的传导物，一根铜质或铝质裸线。其直径相对较大（0.4in㊀）。2 是一层绝缘体，它包围着裸线，以防金属导体碰到第三层材料。3 是第三层材料，通常是一层紧密缠绕的网状导线。这种编织导线起着屏蔽层的作用，保护里层的传导物免受电磁干扰。4 是最外一层，为聚氯乙烯（PVC）或特氟纶（Teflon）外皮，起保护作用。

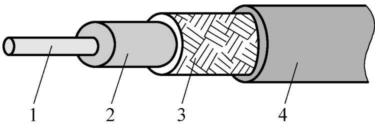


图 1-2　同轴电缆

1—铜质或铝质导体　2—绝缘体

3—网状导线　4—外皮

同轴电缆的这种结构，使它具有高带宽和极好的抗干扰特性。同轴电缆的带宽取决于电缆长度。1km 的电缆可以达到 1～2Gb/s 的数据传输速率。

同轴电缆分为细缆 RG-58 和粗缆 RG-11 两种。

细缆的直径为 0.26cm，适合架设终端设备较为集中的小型以太网络。最大传输距离 185m，超过 185m，信号将严重衰减。

粗缆的直径为 1.27cm，最大传输距离达到 500m。由于直径较粗，强度高，可靠性高，但弹性较差，不适合在室内狭窄的环境内架设，而且 RG-11 连接头的制作方式也相对要复杂些。粗缆适用于网络干线，连接数个由细缆所连接成的网络。

细缆安装则比较简单，造价也较低。由于安装过程要切断电缆，两头必须装上基本网络连接头（BNC），然后接在 T 型连接器两端。

同轴电缆的缺点：一是体积大，细缆的直径就有 3/8in 粗，要占用电缆管道的大量空间；二是不能承受缠结、压力和严重的弯曲；三是成本高。而所有这些缺点正是双绞线所没有的。因此，在现在的局域网环境中，同轴电缆基本已被双绞线所取代。

2. 光纤

光缆通过其中光纤（FiberOpticCable）传输光脉冲信号。其数据传输系统由 3 个部分组成：光源、光纤和检测器，如图 1-3 所示。

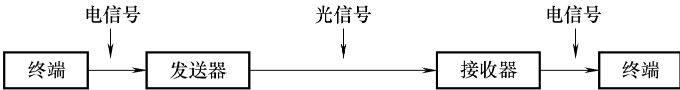


图 1-3　光纤传输系统组成

光源，也即发送器，用发光二极管（LightEmittingDiode，LED）或激光二极管，通电时会发出光脉冲。光纤传输介质是透光的材质，可传输光脉冲。检测器，也即接收器，是光敏二极管，遇光时会产生电脉冲。因此如果在光纤的一端安装一个 LED 或激光二极管，另一端安装一个光敏二极管，一端的电脉冲信号转换为光脉冲后通过光纤可传输到另一端。而另一端经检测则可得到这个电脉冲信号。这样，如果假设出现光脉冲表示“1”，不出现表示“0”，那么，这不就是一个的数据传输系统吗？

这里的关键是，怎样使光传输系统在光纤中传输而不漏光，而这是利用光线从一种介质穿过另一种介质时会发生折射而得到保证的。

㊀　1in＝25.4mm。

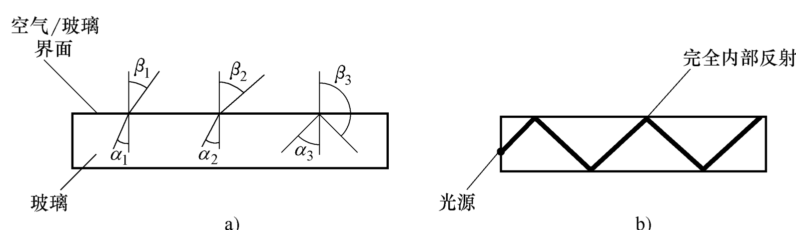


图 1-4　光折射原理

如图 1-4a 所示为光线以不同角度从玻璃入射空气时产生折射的情况。当光线在玻璃上的入射角为 α_1 时，则在空气中的折射角为 β_1。为 α_2 时，为 β_2。这里的 α_1 与 β_1、α_2 与 β_2 是不等的。这就是光通过不同介质时产生的折射。折射时入射角与折射角之间的关系与两种介质折射率有关。具体是

$$n_1 \sin\alpha = n_2 \sin\beta$$

式中，n_1 为第一介质的折射率，光在真空中的传播速度 c 与第一介质中的传播速度 v_1 之比；n_2 为第二介质的折射率，光在真空中的传播速度 c 与第二介质中的传播速度 v_2 之比；α 为入射角；β 为折射角。

折射率与介质的电磁性质及所通过光的波长有关。气体介质的折射率还与温度和压强有关。对各种波长的光，空气折射率都非常接近于 1。如在 20℃、760mmHg[㊀] 高时的折射率为 1.00027。在工程光学中常把空气折射率当做 1，而其他介质的折射率就是对空气的相对折射率。

当光线在玻璃上的入射角 α 继续增大时，折射角 β 也继续加大。当大于某一临界值时，如图 1-4a 中的 α_3，光线将完全反射回玻璃，被完全限制在光纤中。可几乎无损耗地传播，如图 1-4b 所示。

在图 1-4b 中仅给出了一束光线在玻璃内部全反射传播的情况。实际上，任何以大于临界角入射的光线，都将按全反射的方式在介质内传播。

如果纤芯的直径较粗，则光纤中可能有许多种光束沿不同途径同时传播，这种光纤也称为多模光纤（Multi-mode Fiber）；如果将光纤的纤芯直径减小到光波波长大小的时候，则光纤光在光纤中的传播将没有反射，而沿直线传播，这样的光纤称为单模光纤（Single-mode Fiber）。

光纤的主要传播特性为损耗和色散。损耗是光信号在光纤中传输时单位长度的衰减，其单位为 dB/km。色散是到达接收端的时延差，即脉冲宽度，其单位是 μs/km。光纤的损耗会影响传输的中继距离，色散会影响数据传输率，两者都很重要。自 1976 年以来，人们发现 1.3μm 和 1.55μm 波长的光纤可以获得 0.5～0.2dB/km 的衰减率，0.85μm 波长的光纤的衰减为 3dB/km，多模光纤能使 0.85μm 波长的光纤的色散从 400μm/km 减至 10μm/km 以下。在 1.3μm 的波长中，单模光纤的色散近于零，所以单模光纤在使用时，可以同时兼得低损耗和低色散两项优点，无中继的距离可达 50～100km，数据传输率可达 2Gbit/s 以上。

目前在实际中用到的光纤系统能以 2.4Gbit/s 的速率传输 100km，而且不需要中继。多

㊀ 1mmHg = 133.322Pa。

模光纤传播距离要短些，数据传输率也小于单模光纤；但多模光纤价格便宜，并且可以用发光二极管作为光源。单模光纤与多模光纤的比较见表 1-2 所示。

表 1-2　单模光纤与多模光纤的比较

项　目	单模光纤	多模光纤	项　目	单模光纤	多模光纤
距离	长	短	信号衰减	小	大
数据传输率	高	低	端接	较难	较易
光源	激光	发光二极管	造价	高	低

光纤结构如图 1-5 所示。它由包在玻璃管子中的一根或者多根玻璃或者塑料光纤芯线构成，外面的玻璃管子叫做包层。纤芯直径约 5 ~ 75μm，包层的外直径约为 100 ~ 150μm。

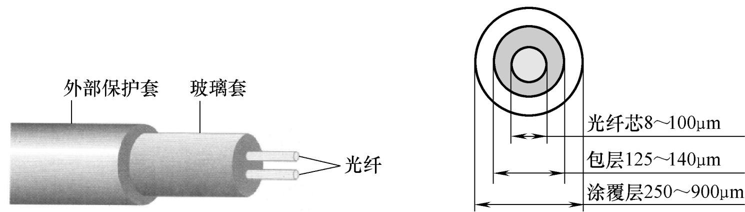


图 1-5　光纤结构

纤芯材料是二氧化硅掺以锗和磷，包层材料是纯二氧化硅。纤芯的折射率比包层的折射率高，以使得光局限在纤芯与包层的界面以内向前传播。

包层之外为涂覆层，由一层或几层聚合物构成，厚度约为 250μm，在光纤的制造过程中就已经涂覆到光纤上。它也是光纤的第一层保护（PrimaryBuffer），目的就是增强光纤的机械强度及保护光纤更好地工作，同时又可以隔离外界水汽的侵蚀。

在涂覆层外面还有一层缓冲保护层。它给光纤提供附加保护。在光缆中这层保护分为紧套管缓冲和松套管缓冲两类。

（1）紧套管缓冲

紧套管是直接在涂覆层外加的一层塑料缓冲材料，约 650μm，与涂覆层合在一起，构成一个 900μm 的缓冲保护层。

紧套管缓冲光纤主要用于室内布线。由于它的尺寸较小，所以使用灵活，并在安装过程中允许有大的弯曲半径，使得安装起来比较容易。

（2）松套管缓冲

松套管缓冲光纤使用塑料套管作为缓冲保护层，套管直径是光纤直径的几倍，在这个大的塑料套管的内部有一根或多根已经有涂覆层保护的光纤。光纤在套管内可以自由活动。这种结构可以防止因缓冲层收缩或扩张而引起破坏，并且可以充当承载元件。

光缆由若干条光纤组成。为增大机械强度和刚性，所组成的光缆还包含有一个或几个加强元件。在光缆被牵引的时侯，加强元件使得光缆有一定的抗拉强度，同时还对光缆有一定的支持保护作用。

光缆加强元件有芳纶砂、钢丝和纤维玻璃棒等 3 种。

此外，光缆护套是光缆的外围部件，它是非金属元件，作用是将其他的光缆部件加固在一起，保护光纤和其他的光缆部件免受损害。

光纤采用光导纤维作传输介质。其优点是频带宽、传输容量大、重量轻、尺寸小、不受电磁干扰和静电干扰、无串音干扰、保密性强、原料丰富，因而已成为当前主要发展的传输介质。但目前的生产成本还较高，且需要高水平的安装技术。所以，其使用还是有所受限制的。

3. 无线传输介质

在自由空间，含地球上的大气层，利用电磁波发送和接收信号用的就是无线传输介质。电磁波以频率划分，图 1-6 所示为各种电磁波与频率的对应关系。

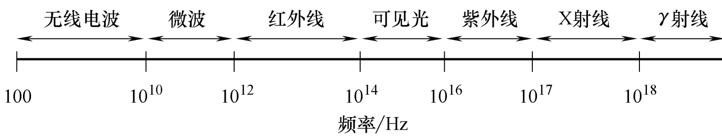


图 1-6　各种电磁波与频率对应关系

从实用角度上讲，可用于通信的电磁波只有无线电波、微波及红外线。利用无线传输介质也还可通过移动通信这样的公用资源连网。

（1）无线电波

网络信号可以通过无线电波进行传输。但网络所使用的信号频率要与无线电台使用频率错开。所以，PLC 网络用得多只是波长短、强度低的短程视线（line-of-sight）传输。但这样传输，信号会被高的物体阻断，因而其传输距离多受限制。

当铺设电缆成本很高且很困难时，使用无线电通信可以大大节省费用，而且易于安装。无线电通信的缺陷是：网络的传输速率低；使用的频率难以控制，易受到其他无线电信号干扰；自然的障碍物（如山峰）也会减弱或干扰信号的传输。

（2）微波

微波系统的工作方式有两种。其一为地面微波，是在两个定向天线间传输信号。这种传输信号的频率为 4～6GHz 和 21～23GHz。卫星微波是在 3 个定向天线间传输信号，3 个天线之一是空间的一颗卫星。这类传输的频率范围为 11～14GHz。

在城市中，采用地面微波进行两个大建筑物之间通信是很好的解决方案。而跨国或在两个洲之间连网，使用卫星通信是较方便的。

这两种类型的微波介质传输速度可达 1～10Mbit/s。再高的网络速度是受限制的。微波通信安装和维护的成本也很高。微波传输还极易受到大气环境、恶劣的天气和电磁干扰（Electromagnetic Interference，EMI）。

（3）红外线

如同电视机用的遥控设备，红外光也可以用作网络通信的介质。红外线可以沿单方向，也可以沿全方位传播。红外线用 LED 是 Light Emitting Diode（发光二极管）产生的，用光敏二极管来接收。传输频率为光的频率——100GHz～1000THz。

与无线电波相同，在电缆连接比较困难或者在移动用户的情况下，红外线技术是一个成本不高的解决方案。但是，它在定向的通信中，数据传输速率仅能达到 16Mbit/s，而在全方位传输时，速率更低，最大仅 1Mbit/s。红外线还不能穿越墙壁，而且强光源也会对红外线通信造成干扰。

表1-3为3种无线传输的优缺点比较。而表1-4为几种传输媒体的特性及其应用，是对本节介绍通信媒体的简要总结。

表1-3 3种无线传输的优缺点比较

	无线电	红外线	微波
优点	·在安装通信电缆比较困难时，是代替布线的一种廉价方法 ·便携通信的一种选择 ·通常不需要许可要求	·在安装通信电缆比较困难时，是代替布线的一种廉价方法 ·信号很难被秘密截取	·在安装通信电缆比较困难时（如要穿越很长的距离），是代替布线的一种方法
缺点	·不适合通信需要高速时 ·易于受军事、无线电爱好者、蜂窝电话等信号源的干扰 ·易于受自然障碍的干扰	·不适合通信需要高速时 ·易于受其他光源的干扰 ·不能穿越墙壁	·不适合通信需要高速时 ·安装维护的成本比较高 ·易于受坏天气、EMI和大气环境的干扰

表1-4 几种传输媒体的特性及其应用

媒体	特性	应用
双绞线	传输距离、带宽和数据速率有限，易受外来电磁场干扰。传输模拟信号时，带宽可达250kHz，衰减约为1dB/km，每隔5～6km需要中继放大；对于数字信号传输，每隔2～3km需要中继放大，传输速率一般小于10Mbit/s	主要应用于传输模拟信号和低速数据信号。在较短的距离内，也可用于中、高速数据传输，如用作局域网中的传输媒体
同轴电缆	带宽较宽，一般可达400MHz，抗干扰能力强。中继间距为1～10km，当采用1.6km间距时，数据速率可达800Mbit/s。其性能主要受衰减、热噪声和互调噪声的限制	1. 长距离电信网干线 2. 局域网 3. 闭路电视系统 4. 短距离高速数据传输
光缆	频带很宽，对各频率的传输损耗和色散几乎相等，中继间隔一般为50～100km或更大，数据传输速率可达1Gbit/s以上。另外，它不受电磁和静电干扰，保密性较好	光纤通信主要采用数字通信方式，用于传输高速数据信号，主要用作各种通信网干线以及大容量高速数据传输媒体
微波	频率范围在300MHz～30GHz之间，它具有传输带宽较宽、传输质量比较平稳等优点，利用卫星中继时，传输距离可以非常大	主要用于长距离电信网干线、卫星通信网以及短距离高速数据通信
无线电波散射	利用地面发射的无线电波在对流层散射而返回地面来进行通信，其频率在100MHz～10GHz之间，通信距离一般为150～400km，最远可达1000km左右，带宽可达数兆赫兹。传输损耗大，衰落现象严重，须采用分集接收技术，通信成本较高	主要用于军事通信，以及边远地区通信
短波	频带较窄，损耗及衰落严重，质量不稳定。但成本低、建设快，通信距离较远（可达上万千米），移动方便	主要用于移动通信、军事通信以及边远地区低速数据和话音通信

1.1.2 网络通信组件

网络通信组件用于站点与通信介质、通信介质与通信介质互连的接口或装置，最重要的是网络接口组件。此外，有时还有数据信号增强及网络互连组件。

1. 网络接口组件

网络接口组件内与主机相连，外与通信介质相连。用于主机与通信介质的连接。

计算机站点的接口组件为集成在主板上的通信接口，或为网络接口插卡。PLC站点的接

口组件是通信处理器，或是集成在 CPU 模块上的通信插件、接口，或是网络接口模块。现场设备站点的接口组件一般是集成在其 CPU 上的通信接口。

简单的站点间的物理连接是链接。如有主机 1、主机 2，其物理连接为主机 1—主机 1 通信接口—通信介质—主机 2 通信接口—主机 2。通过它，可建立直连的通信通道，实现一对一通信。

复杂的是有多个主机，各有各的通信接口，通过通信介质，相互连接，构成较复杂网络与较多的通信通道。在各主机间，都可实现相应的通信。

通信接口与建立的网络类型有关，什么样的网络将有什么样的接口。标准串口网络要使用标准串口，而以太网则要用以太网卡（对计算机）或以太网模块（对 PLC）等。

2. 信号增强组件

数据信号增强组件用于通信介质之间的连接，增强与恢复在介质传输中减弱的信号，以增大信号传输距离或多个站点的集中连接。这类组件很多，如放大器、中继器、集线器、交换机、转换器等。信号增强组件不是网络的站点，只是为增大传输距离而加在传输介质之间。所以，在多数情况下，它不是网络必备的组件。

放大器：用于放大在介质传输中减弱的信号，以增大传输距离。只是它在放大有用信号的同时，也把干扰信号放大了。难以恢复信号“原样”。所以，它不能多次使用。

中继器（Repeater）：也是用于放大在介质传输中减弱的信号。但它不是简单放大，而是先收到信号整形，恢复，然后再放大。如果用于数字信号传输，基本上可使信号恢复“原样”。所以，在数字信号传输中，它可多次使用，可使信号传输的距离更大。

集线器（Hub）：在以太网上使用，以把连接它的所有站点集成在以它为中心的站点上，实现多个站点的连接。它拥有多个不同的端口，可分别与多个站点相连。接收到的任一站点发来数据信号后，都进行恢复、放大，并以广播的方式传送到与集线器连接的其他站点。

此外，集成若干站点的集线器，也可作为站点与另一集成器连接。图 1-7 所示的就是一例。集线器 A 集成 4 台计算机。集线器 B 集成 2 台计算机。作为站点的集线器 A、B 则互为对方的一个站点。

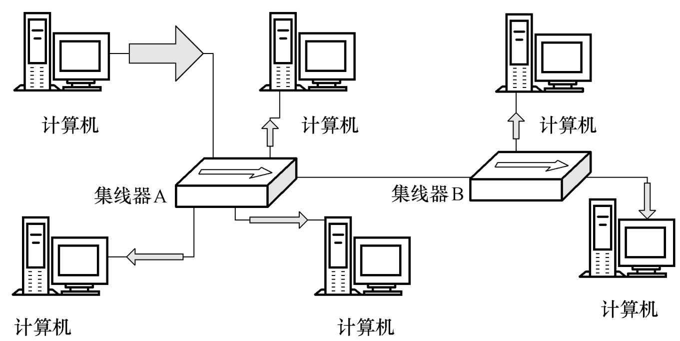


图 1-7　集成若干站点的集线器与另一集成器连接

如果集线器有两个以上端口同时收到数据信号，都要以广播的方式向其他端口传送，就会出现所谓的数据碰撞（Collision）情况。这时，这个传输将是无效的。常出现这样情况将降低网络的数据传输效率。

交换机（Switching）：也是在以太网上使用，又称为交换式集线器，与集线器一样，也是用于多个站点的连接。但集线器功能单一，不能识别数据的目的地址，只能广播转发数据。而交换机功能较强，能识别数据的目的地址，能找准对象有针对性地转发。

这种交换机与电话交换机很相似。一个人给另一个人打电话，要经过电话交换机识别、连接，然后一对一通话。一个站点通过交换机给另一个站点传输数据，交换机收到数据后，也是识别，建立内部连接，然后把所收到的数据转送给目的站点。所不同的是，网络站点是用标明目的站的地址来区分对方，而电话则是通过电话号码来识别对方。

转换器：用以信号转换。种类很多，如光电信号转换器，用以光信号与电信号的相互转换；接口类型转换器，以一种网络类型的接口转换为另一种类型的网络接口；接口特性转换器，用以接口间机械、电气等特性的转换。等等。

在 PLC 网络中使用或不使用这些组件，使用什么组件与网络站点的分布有关，也是网络配置要处理好的一个重要问题。

3. 网络互连组件

计算机网络互连常用的是可连接相邻网络的网桥（Bridge）、路由器（Router）或网关（Gateway）这样的组件。

PLC 网络的互连则多用配置有多个网络接口的 PLC。用它同时与多个网络连接，起到网络互连组件的作用。

用 PLC 作这样的网络互连，多数情况下只是“兼职”，其主要的工作还是用于实现原有的功能。所以，用它作 PLC 网络互连，投资效益较高。在一些特殊情况下，一些专用的 PLC 网络之间互连还真是“非它莫属”。

提示：网络组件的名称很多。同样功能的组件由于生产厂家及应用场合的不同名称可能不同。选用时要仔细了解。

1.1.3　网络拓扑结构

网络拓扑结构指，网络站点之间物理连接的抽象图形，或者是它在物理上的连通性。拓扑结构与传输媒体及媒体访问控制方法的确定紧密相关，涉及网络的可靠性、费用、灵活性、响应时间和吞吐量等问题。PLC 网络拓扑主要有：

1. 两点连接

两点连接也就是站点间链接，比较简单。距离近时，如几十米、几百米，用通信接口、介质直接相连就可以了，如图 1-8a 所示。距离远的可用光纤，也可用电缆但要加中继器。也可通过公网，如电话网，用调制解调器连接，如图 1-8b 所示。后者的连接距离不受地理限制，凡是电话能到达的地方都可连接。此外，还可利用无线调制解调器，通过电波或光波进行连接。

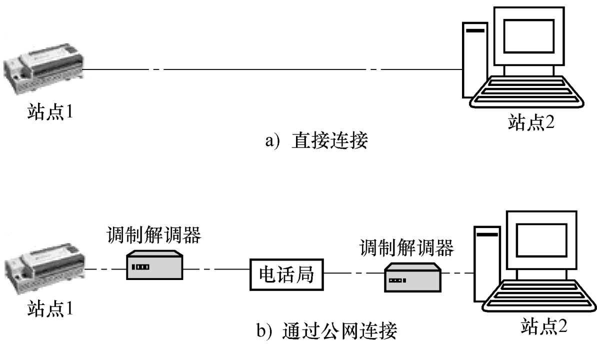


图 1-8　两点连接

在这种点到点的拓扑结构中，没有信道竞争，几乎不存在介质访问权控制问题。

2. 多点连接

多点连接的拓扑结构有星形结构、总线结构、环形结构、树形结构、网状结构及混合结构，如图 1-9 所示。

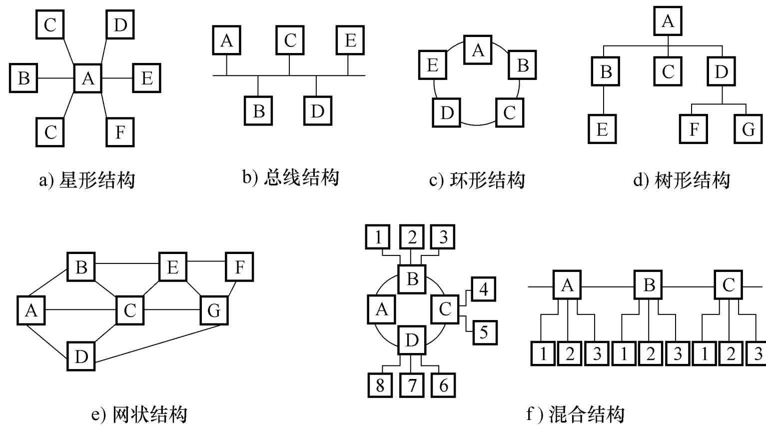


图 1-9　网络结构

（1） 星形结构

这种结构有中心站点，网络上各站点都分别与中心站点连接。图 1-9a 所示为星形结构。它的通信由中心站点管理，并都通过中心站点。如非中心站点间通信，发送数据的站点需要把数据先传输给中心站点，然后再由中心站点把数据转送到目的站点。

在 PLC 连网中，若用一个计算机与多个 PLC 连网，有可能就是这种结构。计算机为其中心站，一切通信都由计算机管理，PLC 与 PLC 通信也要通过计算机。

星形网络的特点是：网络结构简单，便于管理；控制简单，建网容易；网络延迟时间较短，误码率较低；网络共享能力较差；通信线路利用率不高；中央站点负荷太重。

（2） 总线结构

这种结构靠公共传输介质（称为总线）实现各站点的连接，见图 1-9b。所有站点通过硬件接口与总线相连。任何站点都可在总线上发送数据，并可随时在总线上接收数据。

用集线器把所有站点集成在一起，形状上看好像是星形结构，但实际是总线结构。因为连接后各个站点是对等的，没有主从关系。

这种结构比较简单，各站点间可直接进行数据交换，这也是 PLC 连网实现通信所要求的。问题是，仅有一个总线，若在同一时间内有多个站点都在发送数据，那么总线上的数据将相互混淆。其他站点接收的数据到底是什么就很难说了。为此，一定要解决好站点发送数据权的授予问题。

总线结构的优点是简单灵活，是一种很容易建造的网络。多个站点共用一条传输信道，所需电缆数量少，信道利用率高。结构简单又是无源工作，有较高的可靠性。易于扩充，增减用户方便。传输速率也高，可达 1～100Mbit/s。

其缺点是传输距离有限，通信范围受到限制。故障诊断和隔离困难。要有媒体访问控制功能，增加了站点软件和硬件的开销。

（3）环形结构

这种结构网上的所有站点都通过点对点的链路连接，并构成封闭环，如图 1-9c 所示。每一台设备只能和它的一个或两个相邻站点直接通信。要与其他站点通信，信息必须依次经过两者之间的每一个设备。

环形结构可以是单向的，也可以是双向的。双向时，数据能在两个方向上传输。因此一个站点可以和两个邻近站点直接通信。优点一是电缆长度短；二是增减工作站时只需简单连接；三是可用光纤。

环形结构的一个缺点是：当一个站点要往另一个站点发送数据时，它们之间的所有站点都得参与传输。这样，比起总线结构，更多的时间被花在替别的站点转发数据上。而且只要一个站点发生故障，就会导致环中的所有站点无法正常通信。

（4）树形结构

图 1-9d 所示为这种结构。它从总线拓扑演变而来，像一棵倒置的树，顶端是树根，树根以下带分支，每个分支还可带子分支。树根接收各站点发送的数据，然后再广播发送到全网。其优点是易于扩展，故障隔离较容易。缺点是站点对根依赖性太大，若重要的根发生故障，则全网不能正常工作。

我国电话网络即采用树形结构，由五级星形网构成。著名的因特网（Internet）从整体上看也是采用树形结构。图 1-10 所示为某小型校园网基础网络示意图，它也是典型的树形结构。如果有 PLC 站点，只要有相应的接口也可加入。

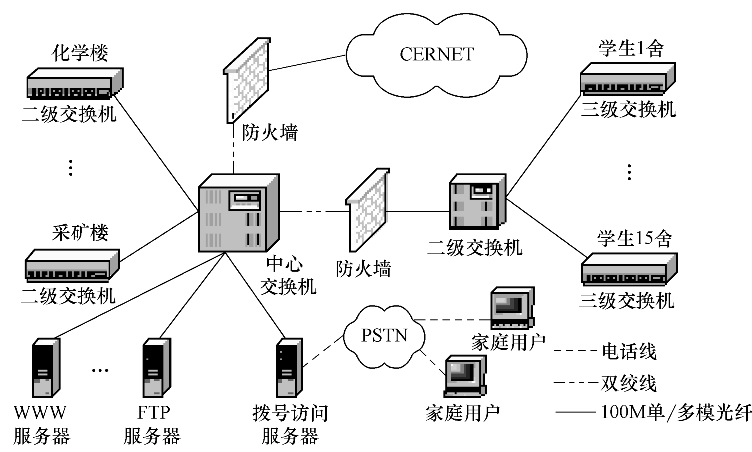


图 1-10　某大学校园网结构示意图

树形网络的主要特点是结构比较简单，成本低。在网络中，任意两个站点之间不产生回路，每个链路都支持双向传输。网络中站点扩充方便灵活，寻找链路路径比较方便。但在这种网络系统中，除叶站点及其相连的链路外，任何一个站点或链路产生的故障都会影响整个网络。

（5）网状结构

图 1-9e 所示为这种结构。最理想的状况是所有站点都能直接相连。这当然很浪费了，也没有必要。多数是重要站点间能直连。网状形结构特点是，网络可靠性高，它的任意两个站点之间，都存在着两条或两条以上的通信路径。这样，当一条路径发生故障时，还可以通

过另一条路径传送。另外，可扩充性好，该网络无论是增加新功能，还是要将另一台新的计算机入网，以形成更大或更新的网络时，都比较方便。网络可建成各种形状，采用多种通信信道，多种传输速率。著名的中国教育科研计算机网络（CERNET）其主干网就是网状结构。

这个网络拓扑结构的特点是，任何城市站点到北京最多仅需相隔一个城市。而任何两个城市之间最多只要相隔两个城市。

这种结构的缺点是结构较复杂，建设成本高。只用于计算机的骨干网络，而 PLC 网络很少有这样的拓扑结构。

（6）混合结构

混合形拓扑是将两种单一拓扑结构混合起来，取两者优点构成的拓扑，如图 1-9f 所示。其优点是故障诊断和隔离方便。易于扩展。安装方便。缺点是需用智能集中器。集中器到各站点的电缆长度会增加。

3. 网络互连

网络互连用的多是用路由组件或网桥的站点实现。其结构很多。可以是上述结构的任一组合。目的都是为了能在网络上的任何站点之间都可物理连接。

1.2　PLC 网络通信技术

关键词：单工、半双工、全双工、线路交换、存储交换、直接电平编码、曼彻斯特编码、差分曼彻斯特编码、4B/5B 编码、面向字符传输、面向位（比特）传输、信号调制解调制、频分多路复用、时分多路复用、波分多路复用、码分多路复用

本节将简要介绍通信方式、通信数据、数字通信、模拟通信及信道复用等有关网络通信技术的基础知识。

1.2.1　通信方式

1. 直接相连的站点之间通信方式

（1）单工（simplex）通信

单工通信包含的环节如图 1-11a 所示，有：

信源，也即发送数据的站点，它通过通信接口（发送口），处理通信数据，并把处理后的数据转换成通信信号，发向通信信道（媒体）；

通信，信号在信道（媒体）上传输；

信宿，也即接收数据站点，通过通信接口（接收口），从媒体上接收通信信号，再转换成数据，并存入缓冲区，供接收站点使用。

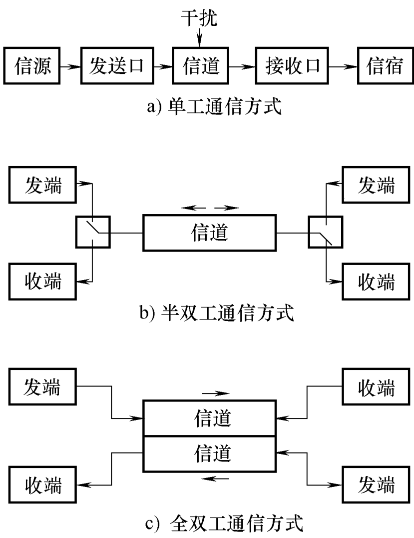
它是单向传输。数据只能从信源站点传输到信宿站点。故称单工通信。有线电视网络传输数据就是用这种方式。这种通信信息不能双方交流，故在 PLC 网络中用得较少。

（2）半双工（halfduplex）通信

见图 1-11b。它的通信接口能按通信要求，适时互换信源与信宿的角色，两个方向都可传输数据。但它在同一时刻，只能朝一个方向进行传输。步话机通信就是用这种方式。计算机、PLC 也常用这种方式通信。

（3）全双工（Fullduplex）通信

见图 1-11c。它的站点同时配备有发送口与接收口，通信通道也配备两个。所以，两个站点可同时双向通信。电话网用的就是这种方式通信。计算机网络、PLC 网络也常使用此方式通信。



a) 单工通信方式

b) 半双工通信方式

c) 全双工通信方式

图 1-11　数据传输过程示意图

（4）广播、多播通信

在半工、全双工方式下，如果有多个站点，也可一个站点广播发送数据，其他所有站点或其中多个接收数据。而哪个站点有权发送数据可以预先指定、实时争抢或按协议轮换。很多计算机、PLC 网络也用这种方式通信。

2. 不直接相连的站点之间通信方式

如果相互通信的站点不直接相连，或不在同一网络中，其通信有两种方式：

（1）线路交换

在通信开始前，必须先建立一条从源站点通到目标站点之间一系列站点的连接线路，即信道，然后再在这条连接的信道上通信。在通信期间，这条信道始终被占用，别的通信无法插入。待这个通信完毕后，才断开连接，释放所占用的信道。在电话网中，用户之间通话，使用的就是线路交换。

线路交换技术有两大优点，第一是传输延迟小，唯一的延迟是物理信号的传播延迟；第二是一旦线路建立，便不会发生冲突。第一个优点得益于一旦建立物理连接，便不再需要交换开销；第二个优点来自于独享物理线路。

线路交换建立连接需要时间，建立连接后数据是否传输都要占据有关资源，所以，网络的利用率较低。当然，这种浪费也有好处，对于占用信道的用户来说，其可靠性和实时响应能力都得到保证。只是一旦出现连接故障，不重新连接，也无法通信。因而通信安全不是太高。

（2）存储转发

在通信开始前，不须先建立一条从源站点通向目标站点之间的连接信道。而是把数据择机发送给与靠近目标站点的相邻站点，相邻站点收到数据后，先存储（暂存），后择机转发给更靠近目标站点的次一相邻站点。依次类推，直到把数据交给目标站点。

存储转发有报文交换与分组交换两种。

报文交换是把要传送的数据当做报文进行传送。它传送的延时较长。如报文较大，中间站点存储的空间可能不符要求，不大可靠。所以用得不多。

分组交换是把要传送的数据先拆分成大小一定的“包”，加上首部的控制信息，组成一个便于在网络上传输的数据分组，然后发送各个分组。目标站点接收到所有分组后，再进行组合，恢复成所传送的数据。

存储转发的信道为动态占用。只有数据在传送的链路才被占用，其余的不被占用（这时这些资源可以让其他用户使用），资源利用率高。特别是分组交换，比较灵活，每个分组还可独立选择发送路径；速度快，可不先建立连接就可发送分组；通信不致瘫痪，因为总是

可找到合适数据传输通路。

图 1-12 所示为线路交换、报文交换及分组交换的图解示意。从图可知，分组交换比报文交换要优越些。

这是因为，在具有多个分组的报文中，中间交换机在接收第二个分组之前，就可以转发已经接收到的第一个分组，即各个分组可以同时在各个站点对之间传送，这样减少了传输延迟，提高了网络的吞吐量。此外，分组交换还提供一定程度的差错检测和代码转换能力。

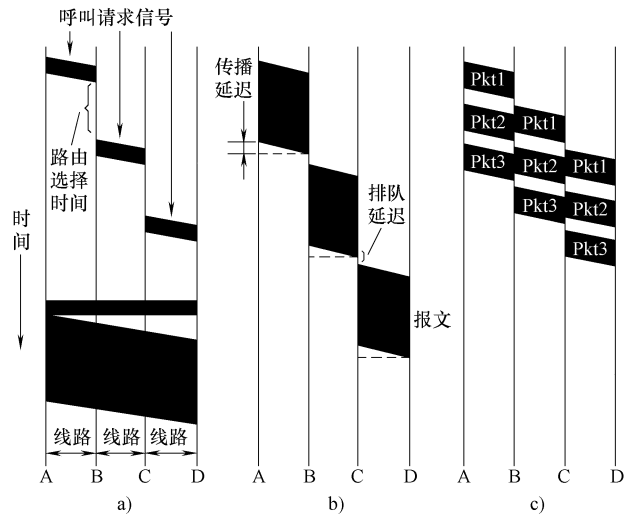


图 1-12　线路交换、报文交换及分组交换图解示意

分组交换的缺点是：分组数据拆分及合成需要管理，同时，每个分组还要另增加首部（标志）信息，通信协议也比较复杂。

分组交换所用的存储转发技术最早用在 ARPANET 网络中。由于它的成功应用，才导致计算机网络的长足发展，以致有今天网络技术这样的成功。然而，存储转发也是古老的技术。实质上讲，通过邮政向远方发信，在相关邮局之间也是一站站存储（接收后再）转发的。

由于分组交换优点突出，所以在 PLC 网络中，不直接相连的站点之间通信，也是用这种方式。

要指出的是，在分组交换中，还有虚电路分组交换。它类似前述的线路交换，如图1-13 所示。在分组发送之前，也要有呼叫的过程，使网络建立一条通往目的站的虚拟（逻辑）通路。然后，一个报文的所有分组都沿着这条通路进行存储转发，不允许站点对任一个分组做单独的处理和另选路径。

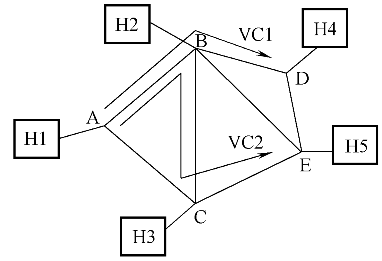


图 1-13　虚电路传输分组交换

在图 1-14 中，假设 H1 站有 3 个分组（P1、P2、P3）要送往 H5 站去。H1 站首先发一个“呼叫请求”，即发送一个特定格式的分组给站点 A，要求连到 H5 站进行通信，以寻找一条合适的路径。站点 A 根据路选原则将呼叫请求分组转发到站点 B，站点 B 又将该分组转发到站点 C，C 站点再将该分组转发到站点 E，最后站点 E 通知 H5 站。这样就建立起一条 H1-A-B-C-E-H5 的逻辑通路。若 H5 站准备好接收报文，可发一个“呼叫接收”分组给站点 E，沿着同一条通路传送到 H1 站，从而 H1 站确认这条通路已经建立，并分配一个“逻辑通道”标识号，记为 VC1。此后 P1、P2、P3 各分组都附上这一标识号，交换网的站点都将它们转发到同一条通路的各链路上传输，这就保证了这些分组一定能沿着同一条通路传输到目的地 H5 站。全部分组到达 H5 站并经装配确认无误后，任一站都可以采取主动发送一个“消除请求”分组来终止这条逻辑通路，具体过程由交换网内部完成。

要注意的是，虚电路分组交换虽然占用了一条端到端的物理线路，但这与线路交换有本质的区别。这里的虚线路标识号只是对逻辑信道的一种编号，并不指某一条物理线路本身。一条物理线路可能被标识为许多逻辑信道编号，为其他分组交换所用。假定主机 H1 还有另一个进程在运行，此进程还想和主机 H4 通信。这时，H1 可再进行一次呼叫，并建立一个虚线路，在图 1-14 中标记为 VC2，它经过 A-B-D 3 个站点。由图可见，链路 A-B 既是 VC1 的链路，也是 VC2 的链路。

要指出的是，非虚拟方式没有呼叫建立过程，但每个分组（或称数据报）均带有完整的目的站的地址信息，独立地选择传输路径，到达目的站的顺序与发送时的顺序可能不一致。而虚线路方式必须通过虚呼叫建立一条虚线路，但每个分组不需要携带完整的地址信息，只需带上虚线路的号码标志，不需要选择路径，均沿虚线路传送，这些分组到达目的站的顺序与发送时的顺序完全一致。非虚线路和虚线路的区别列于表 1-5。

表 1-5　非虚线路与虚线路的区别

	数　据　报	虚　线　路
端到端的连接	不要	必须有
目的站地址	每个分组均有目的站的全地址	仅在连接建立阶段使用
分组的顺序	到达目的站时可能不按发送顺序	总是按发送顺序到达目的站
端到端的差错控制	由用户端主机负责	由通信子网负责
端到端的流量控制	由用户端主机负责	由通信子网负责

1.2.2　通信数据

1. 数据类型

（1）模拟数据

其变化是连续的，可在一定范围内任意取值，表示它用的是模拟信号。语音、图像数据就是模拟数据。

（2）数字数据

其变化是不连续的，如二进制数据只能在 0、1 之间取值，就是数字数据。表示它多用数字信号。

2. 数据转换

模拟数据经采样、量化，可以转换数字数据，并用数字信号表示。PLC 模拟量输入模块要实现的就是这个功能。反之，数字数据经数-模转换也可变为模拟数据，并用模拟量表示。PLC 模拟量输出模块要实现的就是这个功能。

3. 数据表示

数据可通过信号表示。模拟数据表示比较简单，直接用对应的电压或电流大小表示就可以了。而数字数据信号表示则要先编码，然后用与编码对应的信号表示。编码的方法较多，常用的有：

（1）直接电平编码

也称非归零（NRZ，Non-ReturntoZero）表示。它对逻辑 1、0 分别用相同宽度和幅值但极性相反或幅值不同的脉冲电压表示。

NRZ 编码简单。缺点是无法确定一个位的开始和结束，不便于双方保持同步；同时，当信号中包含的逻辑 1、0 个数不相同时，存在直流分量。

为此，为了保持同步，接收方采用了传输速率（波特率）某倍数（如 64 倍、16 倍）的时钟来采样传输信号，如图 1-14 所示。

图用的是 16 倍数的时钟频率。找到起始位后，于时钟的第 8 周期采样。以后为每隔 16 个时钟周期再采样。这样可保证，所采样的 ON 或 OFF 信号，均为接近 ON-OFF 变化周期中心处的信号。效果当然要好得多。

此外，也可使用归零（RZ，Return-to-zeroCode）编码。用这样编码时，在两次输出之间，输出信号都要先归零，如图 1-15 所示。这样，在接收方，从每次收到归零信号时，就可得知时钟信号。

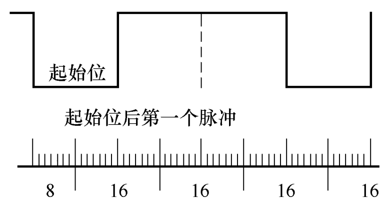


图 1-14　用倍数时钟采样

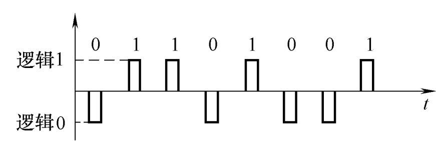


图 1-15　归零编码示意

只是归零码的脉冲较窄，由于存在脉冲宽度与传输频带宽度成反比的关系，可知它在信道上占用的频带较宽。

还有一种编码为不归零就翻向（NRZI，Non Return to Zero Invert）的编码。和 NRZ 的区别就是 NRZI 用信号的翻转代表“0”，信号保持不变代表“1”。图 1-16 给出一个数据流和等同的 NRZI 码流，其中高电平代表数据线上的 J 状态。一串“0”会使得 NRZI 数据每比特周期都会出现跳变，而一串“1”则使得数据中长时间不会出现变化。

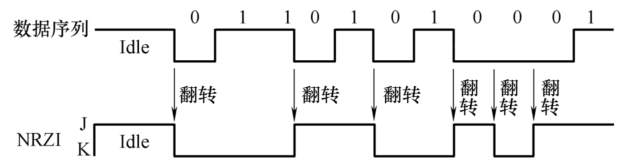


图 1-16　与数据流和等同的 NRZI 码流

这样的编码方式会遇到的问题是：若一直为“1”信号进入时，就会造成数据长时间不翻转。这可能造成读取的时序出错。因此在 NRZI 编码之间，还需执行所谓的位填塞（bits-tuffing）工作。办法是：若原始的串行数据中含有连续 6 个“1”位，就强制插一个“0”，也就是 bit-stuffing。如果传输的数据中有 7 个连续的 1，发送前就会在第 6 个“1”后面强制插入一个“0”，让发送的信号强制出现翻转。接收者接收后只要删除 6 个连续“1”之后的“0”，就可以恢复原始的数据了。USB 口传输数据使用的就是这个编码。

（2）曼彻斯特（Manchester）编码

其特点是每位都有跳变，并用周期中间的不同跳变，表示 ON-OFF。由低跳到高表示“0”或 OFF，反之表示“1”或 ON。

图 1-18 表示的都是“0100101”的不同编码，图 1-17a 为 NRZ 编码，低电平为 0 而高电平为 1。图 1-17b 用曼彻斯特编码，0 为在周期中间处于正的跳变，1 为在周期中间处于负的跳变。而在周期的起始处则为这相应的跳变作准备。

曼彻斯特编码的每个比特位在时钟周期内只占一半，当传输“1”时，在时钟周期的前一半为高电平，后一半为低电平；而传输“0”时正相反。这样，每个时钟周期内必有一次跳变，这种跳变就是位同步信号。

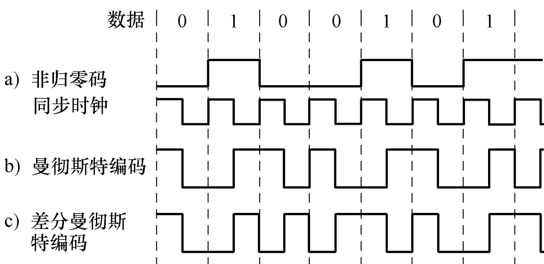


图1-17　基带传输码制

（3）差分曼彻斯特编码（DifferenceManchester）编码

用周期中间的跳变作定时，而值由周期开始处是否跳变确定。开始处若有跳变，表示“0”、OFF，没有跳变，表示“1”、ON。图1-17c就是用差分曼彻斯特编码表示“0100101”的。

差分曼彻斯特编码是曼彻斯特编码的改进。它在每个时钟位的中间都有一次跳变，传输的是“1”还是“0”，是在每个时钟位的开始有无跳变来区分的。这样，差分曼彻斯特编码比曼彻斯特编码的变化要少。

曼彻斯特码和差分曼彻斯特码不含直流分量，包含时钟信息，便于双方同步。著名的10M以太网就是用的曼彻斯特码。Profibus网用的是差分曼彻斯特码。然而，由于这两种编码每个时钟位都必须有一次变化，信号变化频率比不归零编码高，在信道上占用的频带较宽。设备使用效率仅可达到50%左右。

（4）4B/5B编码——快速以太网

这种编码是将欲发送的数据流每4bit作为一个组，然后按照4B/5B编码规则将其转换成相应5bit码。5bit码共有32种组合。实际只使用了24种，其中的16种用做数据符号，其余8种用做控制符号。表1-6列出0～15的4位二进制数对应的4B/5B码。

表1-6　0～15 4位二进制数对应4B/5B码

符号	4位二进制数	4B/5B码	符号	4位二进制数	4B/5B码
0	0 0 0 0	1 1 1 1 0	8	1 0 0 0	1 0 0 1 0
1	0 0 0 1	0 1 0 0 1	9	1 0 0 1	1 0 0 1 1
2	0 0 1 0	1 0 1 0 0	10	1 0 1 0	1 0 1 1 0
3	0 0 1 1	1 0 1 0 1	11	1 0 1 1	1 0 1 1 1
4	0 1 0 0	0 1 0 1 0	12	1 1 0 0	1 1 0 1 0
5	0 1 0 1	0 1 0 0 1	13	1 1 0 1	1 1 0 1 1
6	0 1 1 0	0 1 1 1 0	14	1 1 1 0	1 1 1 0 0
7	0 1 1 1	0 1 1 1 1	15	1 1 1 1	1 1 1 0 1

为了得到信号同步，还可以采用二级编码的方法。即先按4B/5B编码，然后再用NRZI编码。确保5比特编码中至少有2位“0”，从而保证传输的信号至少发生两次跳变，以利于接收端的时钟提取。

使用4B/5B码。对于100Mbit/s的网络只需125MHz的元件就可实现，使设备使用效率提高到80%。所以，在高速以太网及一些光纤网络多使用它。

4. 数据传输

无论是模拟数据还是数字数据，其传输都有两种方法：模拟传输及数字传输。而为了充

分利用信道资源，这两种传输还都可使用信道复用传输。

（1）模拟数据模拟传输

就是模拟数据直接在通信线路传输。在传统的电话网络中（入户使用的为 3 类无屏蔽双绞线）传输语音信号，就是模拟数据模拟传输。由于语音这样的信号带宽不是很大，所以用普通电话信道传输，也不会有太大的减弱及失真。

当然，如果传输距离太大，信号减弱及失真是难免的。为此，在线路中可增加中转器。对模拟传输，这中转器只是简单的信号放大器。用它把衰减的信号放大，恢复至原始的强度。但它在原始信号放大的同时，噪声也放大了。也将恶化信号传输效果。所以，模拟传输只能用于对传输要求不高，传输距离不太大的场合。

（2）数字数据数字传输

经编码后的数字数据为脉冲信号。数字传输就是在线路上，直接传输这个脉冲信号。脉冲信号带宽很大，为了不失真，对线路要求高，不然就很难传输到很长的距离。

数字传输要增大距离也可增加中转器。这中转器则是信号收发处理器。它收到数字信号后，先进行识别，以得出正确的数字数据。然后再用表达这数据的数字信号向远方传输。所以，它的中转器有去除噪声的功能。因而可实现远距离传输。这也是当今远距离网络都使用它的原因。数字传输还可加密，可按自己的要求转换数据与信号间的对应关系。如果其他人不清楚这个关系，即使监听到此信号，也不能得知其中的真实数据或信息含义。只是数字传输对信道特性要求高，需要较多的投入。

（3）数字数据模拟传输。经编码后的数字数据虽为脉冲信号。但传输前可用它调制正弦波信号。这样，也可实现数字信号模拟传输。也可用普通电话信道，可以进行长距离通信，而没有失真。

（4）模拟数据数字传输。模拟数据经采样、量化也可变为数字数据。因而也可用数字传输。而为了远距离传输，这数字化后的数据又可模拟传输。事实上用 Modem 上网，使用 IP 电话就是这样反复的转换过程。

（5）信道复用传输。为了充分利用资源，特别是稀有资源或高性能的信道，往往对信道进行复用，可同时或相当于同时传输多路数据。如无线电广播，利用的信道是电磁场，而用不同信号的频率，就可传输不同的声音数据，使这个稀有的资源可得以复用。再如，有线电视信道是光纤与同轴电缆混用，这两个信道都是复用，因而一个信道可传输多套节目。只是 PLC 网络信道性能大多不是太高，所以复用的场合不多。

1.2.3　数字传输

数字可并行传输，也可串行传输。在串行传输中还有个如何同步以及面向字符与面向比特的问题。数字传输是直接把编码信号通过信道发送给目标站点，也称基带传输。由于信号频带宽，所以传输距离或速率要受限制。以下分别就这些问题作简要讨论。

1. 并行传输与串行传输

在计算机、PLC 及现场设备中，数据的表达、存储、处理都是并行的，即数据的各个位总是同时参与运算或处理。数据传输当然也可是并行的。实际上，各站点内部以总线形式的部件间的数据传输，就是并行传输。为了节省资源用的更多的是串行传输。

（1）并行传输

并行传输，可以字或字节为单位传输。这单位也叫数据宽度。图 1-18 所示为并行传输的示意。从图可知，它除了数据线外，还要有一些控制信号线，如这里的数据准备好、选通等。并行传输速度快，但用的通信线多，成本高，不宜长距离传输，多只用在计算机内部或PLC 内部部件或模块间交换数据。此外，计算机连接打印机也多用它。

PLC 与 PLC 通信，如果交换的数据不多，最简单的通信方法，也可互相把自己的输出信号，作为对方的输入信号。这样处理，还可不用什么选通信号。只是如此并行传输通信距离不长，而且开销也太大，一般不用。

（2）串行传输

数据在信号线上一位一位地进行传输，每一位数据都占据一个固定的时间长度（T）。如图 1-19 所示，如一个字节有 8 位，则至少要传 8 次才可把一个字节传出去。

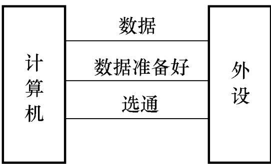


图 1-18　并行传输

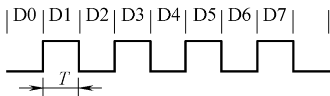


图 1-19　串行数据传送示意

串行传输使用的数据线少。尽管串行传输要多花费些时间，但如果数据传输速率很高，这个时间的增加是有限的。以这种时间的多花费去取得数据线的减少还是很合算的。因而计算机、PLC 网络传输数据都是用串行传输。

2. 数字传输同步

串行一位一位传输数据是分时进行的。为了确保发送方发送的数据能被接收方正确接收，数据发送与数据接收应该协调好，这也就是这里讲的数据通信同步。

最简单的同步方法是，在发送数据的同时，也发送时钟信号。如图 1-20 所示，接收方在接收数据的同时，也接收时钟信号，并依时钟给定的时刻采集数据。

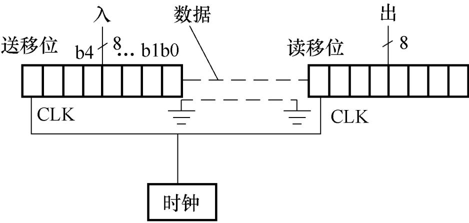


图 1-20　同步方式传输

但是，这样同步方式传输数据，系统比较复杂，计算机网络、PLC 网络基本不用。较实际的解决数据通信同步的办法有两个：

一是在数据信号中不含时钟信号，而靠发送、接收双方设定相同的工作速率，即波特率及数据格式等保证同步。但是毕竟通信双方是两个主机，即使设定的速率相同，时间长了，同步将难以保证。为此，传输数据的每一帧（一组二进制数据）的起始处，都加有起始标志。对方接到起始标志后，再按设定的速率接收数据。这样，即使双方稍有一些速率差别，经过每一帧开始时所作的核对，双方工作同步还是有保证的。

二是使用合适的数据编码，可在数据信号中自包含有时钟信号。这样，在发送方发送数据的同时，也就发送了时钟信号。接收方接收到数据时，先从中提取时钟信号，然后用时钟

信号的节拍实现与发送方工作同步。上述曼彻斯特编码和差分曼彻斯特编码就包含时钟信息，可用以同步。也正因为它的数据多使用含有时钟信号的编码，所以有时也称之为内同步。

当然，更可靠的同步是两者兼用。

3. 面向字符传输与面向位（比特）传输

同样串行传输还有面向字符与面向比特之分。

（1）面向字符传输

它是一个一个字符传输。一个字符一般只有 10 位左右。其中先是起始位，接着为若干数据位，再或为某种校验位或无校验位，最后为停止位。而一个这样的字符到底有多少位以及其中的具体组成，则取决于双方的通信约定，即具体的通信协议。

运用这种传输，不管传输多个数据，都要先把数据以上述字符为单位作划分，然后以这样的字符一个一个传向对方。

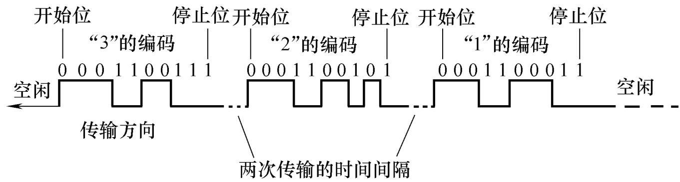


图 1-21　面向字符传输

图 1-21 所示为一个面向字符传输的实例。该图示的是传输数据“321”。虽然传输的是连续 3 个数。但面向字符的传输总是一个一个字符分开传（字符之间的间隔是任意的）。从图知，先是传输字符 3，接着传输 2，最后传输 1。

而在传输字符时，首先是起始位（这里的设定 1 为低电平，0 为高电平，用的是负逻辑），之后为数据位。这里的数据位为 8 位。数据的最高位先传，依次为较低位，最后为最低位。如传输字符 3，则要传 8 位，即 00110011（3 的 ASCII 码二进制值）。数据位之后为停止位（本例无校验位），再就是停止位（输出 1、低电平）。而且，每传输一个字符总是要停止一小段时间，使线路处空闲状态，即输出 1、低电平。各个位之间的时间间隔为传输的速率，即每秒传输多少位（bit）的倒数。接收与发送双方必须预先约定好，并靠各自的硬件及软件保证。

面向字符传输也称异步传输。在一个字符的传输过程中，收发双方基本保持同步。这里所谓异步只是指字符间隔的不确定性。所说的基本同步，是指双方的同步并不基于同一个时钟，会有一定的差异，位数越多，差异越明显。但在异步传输中，每次只传一个字符，每次都进行同步关系的校正，不会造成误差积累。

面向字符传输在传送每个字符时都要传送起始、停止位，字符间还有等待时间，所以，效率低、耗时多。但它对时钟要求不高，容易实现同步传送。计算机、PLC 及现场设备间使用标准通信串口通信，用的都是面向字符的传送。

（2）面向比特传输

它不是以字符为单位传送，而是以一大批位组成的帧传送，一个帧有几十位、几百位。帧具体有多少数据，其中含有什么信息，通信双方要进行约定。

图 1-22 所示为面向位的传输示意。站点 1 为发送方，站点 2 为接收方。在发送的数据帧中，先是 Syn（同步位），接着为 Control（控制位），紧接着为 Data（数据位），再为 Error（校验位），最后为 End（终结位）。

这里 Syn 为起始字节，如有的为 01111110 一个字节、8 位二进制串，表示数据到来，提示对方要做好接收数据准备。Control 为控制字或字节，指明发送及接收地址、帧的长度等信息。Data 为要传送的数据位，是连续的字或字节，即一大批二进制位。Error 为校验字。它按一定算法对所发数据逐位计算后得出的校验码。接收方在收到数据时，也收到此校验码。接收方在收到全部数据后，对校验码之前的数据也作校验计算，然后与所收到的校验码进行比较，看其是否一致？并根据比较结果作相应处理，如要求对方重发或向用户提示等。End 为终结字节，表示这一帧数据传送结束。

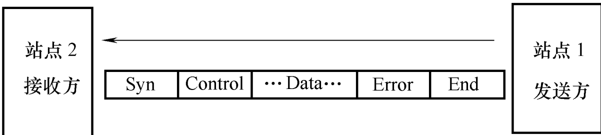


图 1-22 面向位的传输

很显然，使用面向位传送时，帧的具体格式，通信各方一定要先做好约定，各方都按约定处理。否则数据将无法正确传送。

面向比特传输也称同步传输。以上介绍的是帧同步。还有可用位同步。在传送数据流的过程中，发收双方对每一位数据都要准确地保持同步。这可在发送端和接收端间设置专门的时钟线。这叫做外同步，比如 I^2C 总线采用的就是外同步。也还可在数据传输中嵌入同步时钟，如曼彻斯特编码，这叫做内同步。

与面向字符传输相比，它不是每个字符都要有起止位，也没有停止等待，所以传送效率高，适合于大数据量的传送。但面向比特传送的数据最好使用含有时钟信号的编码，以确保同步。

4. 数字传输限制

直接数字信号传输是基带传输。其最高传输距离或速率总是受信道的特性限制的。这是因为从傅里叶分析可知，任何周期信号总是由可以分解为常量信号分量及一系列频率不同、相位不同、振幅不同的正弦信号分量。图 1-23 所示为数字信号傅里叶分析示意。

图 1-23a 所示为二进制数 011000010 的信号波形。周期为 T。其傅里叶分析后列出的谐波共 15 个（未全部列出）。其中 1 为周期为 T 的谐波的振幅，2 为周期为 $T/2$ 的谐波振幅，3 为周期为 $T/3$ 的谐波的振幅……余类推。总的看周期越短，即频率越高，谐波的振幅也越小。

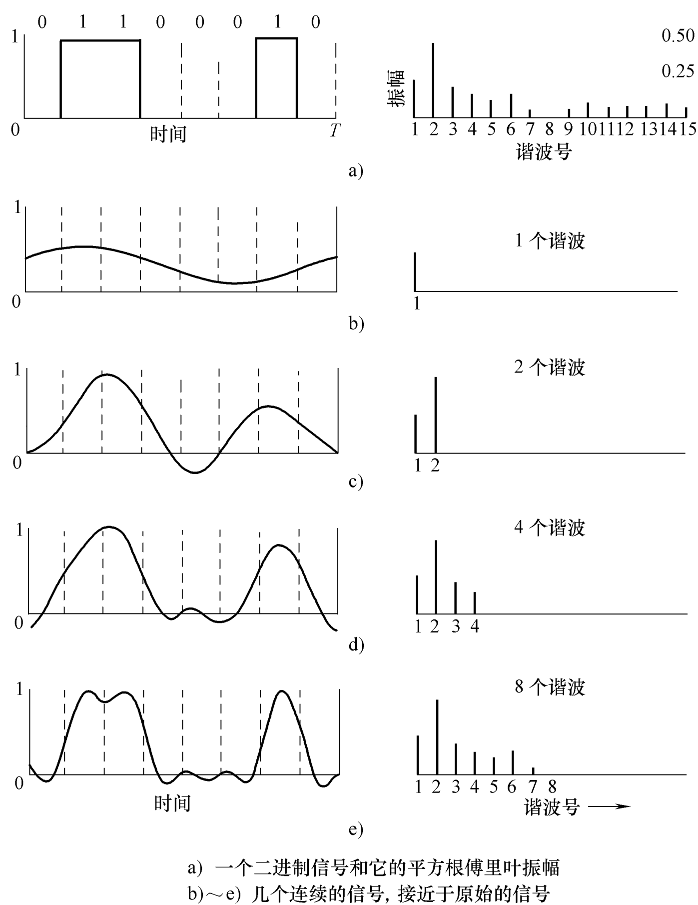
图 1-23b 所示为仅传送一次谐波的波形。这个波形显然与实际波形相差很远。该图 1-23c 所示为仅传送 1 次与 2 次谐波的波形。这个波形显然与实际波形还是相差很远。直到图 1-23e 所示为传送 1 次到 8 次谐波。这个波形就与实际波形相差不大了。这说明，为了保证数字信号能正确传输，直到 8 次所有谐波都必须传送。而可传送谐波数 n 与信道带宽 F 及信号周期 T 有如下关系：

$$n/T < F$$

即

$$n < FT$$

而这里 T 又与二进制数传送的比特率有关。本例每个波形传送 8 位二进制数。所以其比特率为 $8/T$。对普通电话信道最大带宽，即 F，一般为 3000Hz，那么可计算出各个比特率下，可发送的谐波数 n。表 1-7 列出的就是这个关系。



a）一个二进制信号和它的平方根傅里叶振幅
b)～e）几个连续的信号，接近于原始的信号

图 1-23 数字信号傅里叶分析示意

表 1-7 比特率与谐波数关系

bit/s	发送的谐波数	bit/s	发送的谐波数
300	80	4800	5
600	40	9600	2
1200	20	19200	1
2400	10		

从表 1-7 可知，如果比特率达 4800bit/s，那么只能发送 5 个谐波。再高就更少。说明普通电话线路，如果基带传送，比特率不能超过 4800bit/s。当然，如果传输距离短，或不用普通电话线路，就另当别论了。

1.2.4 模拟传输

1. 信号调制解调制

为了克服数字传输的限制，数字数据也可用模拟传输。办法是用数字信号对模拟信号（1000～2000Hz 的正弦信号）进行调制。调制后传输。目的站点收到这个调制的模拟信号后，经过解调，可还原为数字信号。有 1 位、2 位、3 位等多种二进数调制。

（1）1 位二进制数调制

可用0、1 分别进行幅度调制、相位调制或频率调制，如图 1-24 所示。

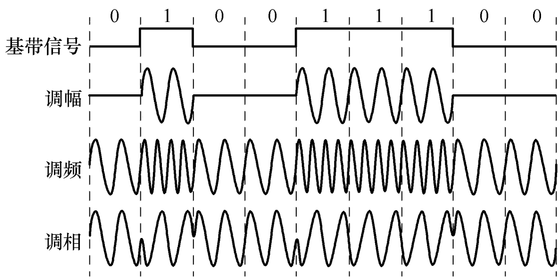


图 1-24　宽带传输码制

如图，调幅（Amplitude Modulation，AM 或 Amplitude Shift Keying，ASK），幅度 0 代表“0”，反之为“1”。调频（Frequency Modulation，FM），也称移频键控（Frequency Shift Keying，FSK），“1”代表频率高，“0”代表频率低。调相（Phase Modulation，PM 或 Phase Shift Keying，PSK）“0”代表初相位为 0°、“1”代表初相位为 180°，而信号的频率及幅值不变，这也称绝对调相。此外，还有相对调相，靠相移调制，“1”时初改变，“0”时保持不变。

这 3 种调制，ASK 抗干扰差，PSK 最好。而 FSK 用得较少。

调制的逆过程，即把已调制的信号还原为 ON-OFF（0、1）信号，称为解调。调制、解调通常用调制解调器，即 Modem 实现。

把数字信号做了调制，对通信信道要求就不必太高了。就可以在普通的电话网络中进行长距离传输。这也是常要用到调制解调器的原因。

（2）两位二进制数

即 4 个信号等级的调制。最方便的是用调相。用同一频率、同一幅值，但初相位不同的 4 个正弦波，表示两位二进制数的不同值。如用初相位 45°表示 00，用初相位 135°表示 01，用初相位 225°表示 10，用初相位 315°表示 11。

这样调制一个信号波形也称码元，可传输 4 个等级的信号，代表 2 位二进制数据。这样，使用同样的信号传输速率，即波特率，可得到加倍的比特率（二进制信号传输率）。这种技术也称正交相移键控（Quadrature Phase Shift Keying QPSK）。

图 1-25a 所示的为幅值相同，但相位不同的 4 个点分别表示两位二进制数的不同值。

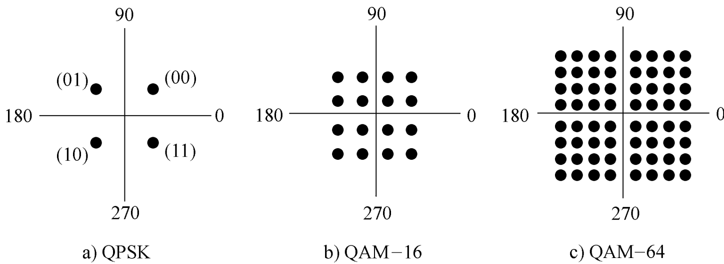


图 1-25　16 及 64 等级振幅相位调制组合星座图

（3）n 位二进制调制

n 位二进制数有 2^n 值。

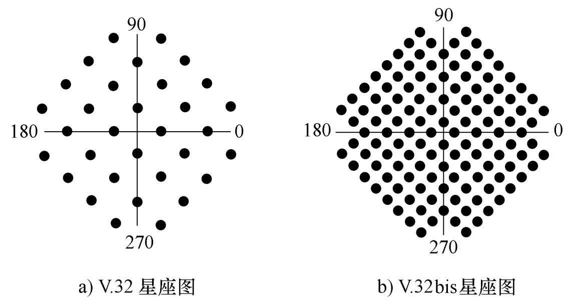
如果不仅用多个相位调制，还用多个幅值调制，即正交振幅调制（Quadrature Amplitude

Modulation，QAM)，可实现更多信号等级。

图1-25b、c所示分别为16（4位二进制数据）及64（6位二进制数据）等级振幅相位调制组合，这个图形也称星座图（Constellation Diagram)。

每个高速调制解调器都有自身的星座图。也只有相同的星座图的Modem才能通信。信号等级太多，可能由于噪声影响而出现信号出错。为此，可增加校验位。如4位二进数，用5位表示。其中一位用作校验。如V.32调制解调器标准，就用了32个星座点，但只传输4个二进制数据。这里多余的一位就是校验位。它的波特率为2400，但比特率为9600。

图1-26b所示为V.32bis的星座图。它用了128个星座点，但只传输6个二进制数据。考虑到校验需要。它的波特率为2400，但比特率为14400。表1-8所示为常用的几种Modem标准，它规定了所采用的调制方式以及所支持的数据传输率。相对图1-25，图1-26旋转了90°，这是为了工程实现的方便。本质上两个图是一样的。



a) V.32 星座图　　b) V.32bis星座图

图1-26　V.32 V.32bis Modem 星座图

表1-8　常用Modem标准

版　　本	特　　性	版　　本	特　　性
V.32	4(1)×2400=9600bit/s	V.34bis	14×2400=33600bit/s
V.32bis	6(1)×2400=14400bit/s	V.90	7×8000=56000bit/s
V.34	12×2400=28800bit/s		

注：括号中1为校验位。

此外，为了提高Modem的传输速度和有效数据传输率，目前许多Modem都采用数据压缩和差错控制技术。数据压缩指的是发送端的Modem在发送数据以前先将数据进行压缩，而接收端的Modem收到数据后再把数据还原，从而提高了Modem的有效传输速率。

2. 最高速率限制

数字传输速率受限制的，模拟传输速率也是受限制的。早在1924年，美国AT&T公司的工程师奈奎斯特（Henry Nyquist）针对有限带宽、无噪声的信道，提出计算其最大数据传输率的奈奎斯特定理。即

$$\text{数据传输速率(bit/s)} = 2H\log_2 V$$

式中，H为信道带宽；V信号的离散等级。例如信道带宽为3kHz，分为两个等级时，传输速率只能为6000bit/s。当然，如果多分等级，则传输速率可相应提高。

然而在实际条件下，信号等级不能无限增加，否则由于干扰而造成相邻等级信号无法区分。所以，实际信号传输速率还要受香农（Shannon）定理限制。即

$$\text{最大数据传输速率(bit/s)} = H\log_2(1+S/N)$$

式中，H为信道带宽，S/N为信道的信（号与）噪（声之）比。多数情况下，信噪比用分贝（dB）表示。即

$$\text{信噪比(dB)} = 10\log_{10} S/N$$

这样如果给出的是 dB 信道比，那要先换算成 S/N 后再计算。如普通电话信道，其带宽为 3000Hz，信噪比（dB）为 30。那么它的最大数据传输速率为

$$\begin{aligned}\text{最大数据传输速率(bit/s)} &= H\log_2(1+S/N)\\ &= 3500\log_2(1+1000)\\ &\approx 35000\end{aligned}$$

这是它的最大传输速率。实际上比它还要低些。

香农公式告诉我们，若要得到无限大的信息传输速率，只有两个办法：要么使用无限大的传输带宽（这显然不可能），要么使信号的信噪比为无限大，即采用没有噪声的传输信道或使用无限大的发送功率（当然这些也都是不可能的）。也就是说，信号的传输速率总是要受限制的。

1.2.5 通道复用

高质量的通信通道，特别是通信干线，建设所需费用很贵，可传输宽带很大的信号。为了充分利用这个资源，可在这个通道上建立多个信道，各自传输各自的数据。这也称通道复用。这里复用的要点是，在发送端将多路信号进行组合，然后在一个通道上传输，接收端再将复合信号分离出来。常用复用有：

1. 频分多路复用

频分多路复用（Frequency-Division Multiplexing，FDM）用于模拟信号传输。无线电视和无线广播所用的空间通信通道，就是典型频分复用。同一传播空间可传送很多频率不同的信号。图 1-27 所示为它的工作原理。

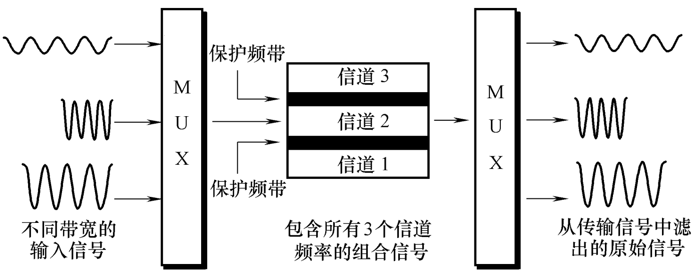


图 1-27 频分多路复用

这里的关键要有多路复用器（MUX）。它接收多个单元被调制的模拟信号（每个信号有自己的带宽），并把这些信号组合成为更大带宽的复合信号。当这个复合信号传输到目标站时，被另一个多路复用器接收。它使用一个带通滤波器把各个独立的调制信号分离开来。接着信号再被解调，并恢复成原始信号。而且在相邻信道间还有保护频带（Guard Band），以防止相邻信道的相互干涉。

家庭用的互联网宽带电话网接入技术也是频分复用。有了它，使用同一电话线，可做到，既可通电话，又能上互联网，两不耽误。

2. 时分多路复用

时分多路复用（Time-Division Multiplexing，TDM）把许多输入信号结合起来，并一起传

输出去。但 TDM 技术用于数字信号。它保持了各信号物理独立性，只是逻辑结合在一起。图 1-28 所示为 TDM 原理。

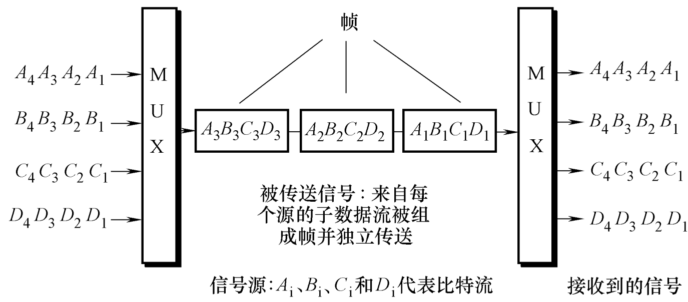


图 1-28　时分多路复用

这里假设 A_i、B_i、C_i 和 D_i（$i=1, 2, 3\cdots$）分别表示来自不同源的数据。先暂存在多路复用器的相应缓冲区中。多路复用器扫描每个缓冲区，从每个区中取出数据放入一个帧中，然后把这个帧发送出去。当在这样做的同时，它重新扫描输入缓冲区，寻找到达的新数据，开始组建下一个帧。如果定时准确的话，它将及时地建好新的帧，并紧接着前面一个帧，把它发送出去。这一过程使得输出线总是保持有效状态，从而使线路的容量得到充分的利用。

如图 1-30 所示，数据 A_1、B_1、C_1 和 D_1 分开存储。多路复用器把它们组合在一个帧中，然后发送出去。紧接着它组合 A_2、B_2、C_2 和 D_2，再行发送。这一过程一直持续到所有数据发送完毕为止。

多路复用器的设计部分地取决于输入输出传输的速度。比如说，如果前面的帧还没有传输出去，各输入源的数据就已经相继到达，多路复用器就必须以快于运送帧的速度产生帧。如果多路复用器没有足够的容量存储多余的帧，它们就会丢失。所以不应供给多路复用器超过它转运能力的数据。另一方面，如果比特源到达的速度太慢，多路复用器在发完前一个帧以后就不得不等待足够的数据到达以组成新帧。这段时间的输出线路处于空闲状态，其容量没有得到充分的利用。

理想的情况是总的输入速度（所有输入源的速度之和）等于输出速度。然而这也是不那么容易。为此开发有如统计复用等多种技术。但基本原理还都是相同的。

3. 波分多路复用

波分多路复用（Wavelength-Division Multiplexing，WDM）用于光纤通道，其实质与频分多路复用是相同的。只是光信号频率很高，波长较短，用波长便于表达。图 1-29 所示为它的工作原理。

这里有 4 个波段的光纤 λ_1、λ_2、λ_3、λ_4，各有其光谱。输入给组合器，后被合成为复合光纤信号。目标端接收此信号后，其分离器又把它分解成各个波长光谱的信号。

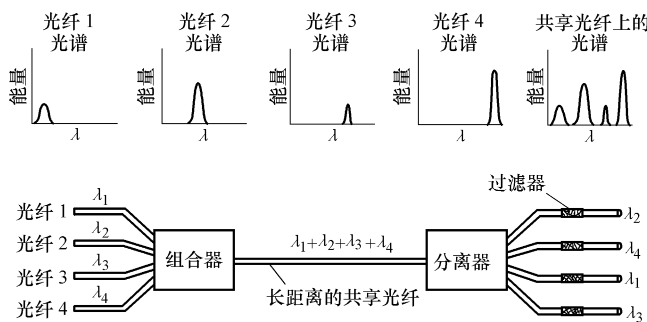


图 1-29　波分多路复用

WDM 技术是在 1990 年前后发明的，发展很快。第一个商用系统有 8 个信道，带宽为 2.5Gbit/s。到了 2001 年就有 96 个信道，每

条信道带宽10Gbit/s，总带宽960Gbit/s的产品。如果信道更多，波长的间隔非常接近（如0.1nm），也称为DWDM，即密集（Dense）WDM。

此外，新的发展还有全光放大器。以前，每100km就必须分离出所有信道的信号，并将其转换成电信号。然后再整形、放大，重新又转换为光信号，并再组合在一起向前传输。而有了全光放大器只需每1000km处理组合的信号，不需多次进行光电转换了。

4. 码分多路复用

码分多路复用CDM，又称码分多址（Code Division Multiple Access，CDMA），传输的信号都加有各自特定的标识码，接收端将根据不同的标识码来区分公共信道上的传输信息。只有标识码或地址码完全一致的情况下传输信息才会被接收。

其具体处理是，每比特时间被分成*m*个更短的时间槽，称为码片（Chip），通常情况下每比特有64或128个码片。每个站点（信道）被指定一个唯一的*m*位的代码或码片序列。当发送1时站点就发送码片序列，发送0时就发送码片序列的反码。当两个或多个站点同时发送时，各路数据在信道中被线性相加。为了从信道中分离出各路信号，要求各个站点的码片序列是相互正交的。

如加入用S和T分别表示两个不同的码片序列，用！S和！T表示各自码片序列的反码，那么S·T=0，S·！T=0，S·S=1，S·！S=－1等关系应成立。当某个站点想要接收站点X发送的数据时，首先必须知道X的码片序列（设为S）；假如从信道中收到的和矢量为P，那么通过计算S·P的值就可以提取出X发送的数据：S·P=0说明X没有发送数据；S·P=1说明X发送了1；S·P=－1说明X发送了0。

此外，还有一些其他的复用技术，如极化波复用和空分复用等。这里就不多赘述了。

1.3　网络结构模型与相应协议

关键词：OSI模型、物理层、数据链路层、网络层、传输层、会话层、表示层、应用层、TCP/IP模型、企业网络标准模型、企业网络事实模型

从上两节的讨论可知，仅仅把网络站点进行物理连接及数据通信，要处理的问题就很多，解决的方案也很多。如果考虑到通信前后的数据处理及与站点之间进程的衔接，要处理的问题就更多，解决的方案也更多。这里的关键是要做好相关约定。这些约定也就是协议，一般含有一些语义、语法、规则等。这里的语义为协议元素含义的解释，也即“讲什么”；语法为协议元素表达的格式，也即“怎么讲”；规则为根据通信中各事件的因果关系规定其执行顺序。有了这些共同约定的语法、语义及规则，通信双方相互操作或交换数据才有可能。

问题的困难还在于网络的各个站点可能是异质的。同样是计算机，类型不同，差别很大。而PLC网络还有PLC及现场设备站点。其类型、规格更是多种多样。如考虑生产厂家不同，差别就更大。各方差异这么大，要做的约定头绪很多，很难实施！

为此，较好的解决方案先是在结构上把网络分割开，划分为若干层，并规定各层的功能及相邻层之间的关系，以建立网络结构体系。具体办法是，把每个计算机互连的功能划分成定义明确的层次，规定同层次进程通信的协议及相邻层之间的接口及服务。这样，用抽象的

原理分层，把复杂问题简化，便于实现，易于维护，灵活性也好，还便于标准化，即使不同质的对象，也就便于处理了。

这里主要用了两个方法：系统抽象及系统模块化。系统抽象是，根据网络互连的公共特性，建立系统模型。这样，可避免涉及具体机型和技术实现细节，也可避免技术进步对互连标准的影响。系统模块化是，根据网络的组织和功能将网络划分成定义明确的层次，然后定义层间的接口以及每层提供的功能和服务，最后定义每层必须遵守的协议。其目的就是用功能上等价的模型代替实际系统。

在计算机网络中，这样分层也称网络结构。有很多结构模型。但影响最大的有两个模型。即 OSI 模型及 TCP/IP 模型。

1.3.1 OSI/RM 模型与相应协议

OSI 模型是国际标准化组织在 1980 年 12 月发表的第一个开放系统互连参考模型（Open Systems Interconnection/Reference Model，OSI/RM）的建议书中提出的。1983 年它被正式批准为国际标准，即著名的 ISO 7498 国际标准。通常人们也将它称为 OSI 参考模型，并记为 OSI/RM，有时简称为 OSI。我国相应的国家标准是 GB/T 9387—1995～1998。

在参考模型中，每个实体和另一个系统的同等实体按协议进行通信；而一个系统中上下层之间的通信通过接口进行，并用服务访问点 SAP 来定义接口。

OSI/RM 模型将网络结构划分为 7 层，自下而上分别为：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。对每一层均规定有具体的功能，并对相邻层之间的关系也作了界定。

以下对这 7 层分别作简要介绍。

1. 物理层（Physical Layer）

物理层是 OSI 网络模型的最底层，规定了不同种类传输设备、传输媒介如何将数字信号从一端传送到另一端，而不管传送的是什么数据，是建立网络的物质基础。但具体的物理媒体并不在 OSI 的 7 层之内。有人把物理媒体当做第 0 层，因为它的位置处在物理层的下面。

物理层的功能是与物理媒体配合构建通信信道，负责站点间的物理连接及实际的信号传输，以便透明地传送比特流。在物理层上所传数据的单位是比特。这里的“透明”含义是，某个实际的物体看起来好像没有一样。“透明地传送比特流”则表示经实际电路传送，比特流没有变化，即“比特流”看不见这个电路。

物理层定义了为建立、维护和拆除物理链路所需的机械的、电气的、功能的和规程的特性。具体涉及接口规格、“0”、“1”信号的表示及其特性、收发双方的协调等内容。本章第 2 节讨论的基本上都是物理层要处理的问题及可能采取的解决方案。

物理层的这些规定要使用相关标准或协议予以协调，它的标准或协议早在 OSI/TC97/C16 分技术委员会成立之前就已制定并在执行了。例如，RS-232C、RS-422A、RS-485 及 FDDI 等。而 OSI 也制定了一些标准并采用了一些已有的成果。其中一些重要的标准如下：

ISO 2110 称为“数据通信——25 芯 DTE/DCE 接口连接器和插针分配”。它与 EIA（美国电子工业协会）的“RS-232-C”标准基本兼容。

ISO 2593 称为“数据通信——34 芯 DTE/DCE——接口连接器和插针分配”。

ISO 4092 称为“数据通信——37 芯 DTE/DEC——接口连接器和插针分配”。与 EIA 的

“RS-449” 标准兼容。

CCITTV. 24 称为“数据终端设备（DTE）和数据电路终接设备之间的接口电路定义表”。其功能与 EIARS-232-C 及 RS-449 兼容于 100 序列线上。

物理层的媒体包括架空明线、平衡电缆、光纤、无线信道等。各种粗、细同轴电缆、T 型接、插头，接收器，发送器，中继器等都属物理层的媒体和连接器。其常用的设备还有重复器（Repeater）、集线器（Hub）、编码解码器、传输介质连接器等，这些可用以信号转发和增强。

2. 数据链路层（DataLink Layer）

数据链路层建立在物理层之上，并为网络层提供数据传送服务。站点间建立物理连接，只是为通信创造物质条件。而进行通信，一般还有建立通信联络、数据传送，然后拆除通信联络这些过程。数据链路层的功能就是针对这些过程，组织帧、进行帧差错检查及控制数据传送流量，确保直接相连站点之间数据尽可能地可靠传输。

帧是数据传送的逻辑单位。每一帧一般包含有同步信息、地址信息、所传送数据以及差错控制信息。有的还有流量控制信息。

在传送数据时，若接收站点检测到所传数据中有差错，如需要及可能，还要通知发方重发这一帧，直到这一帧正确无误地到达接收站点为止。流量控制是控制发送方是否继续发送或停止发送。目的是确保接收方能正确处理所接收到的数据，而不致丢失。这样，链路层就把一条有可能出差错的实际链路转变成让网络层向下看起来好像是一条尽可能不出差错的链路。

数据链路层的常用标准主要有：

1）ISO 1745—1975“信息处理　数据通信系统基本模式控制程序”，是一种面向字符的标准。它与 ISO 1155、ISO 1177、ISO 2626 和 ISO 2629 等标准配合，可形成多种链路控制和数据传输方式。

2）ISO 3309—1984（HDLC 帧结构）、ISO 4335—1984（HDLC 规程要素）和 ISO 7809—1984（HDLC 规程类型汇编），都是面向比特的标准，把这三者组合也称为 HDLC（高级链路控制规程）。

3）ISO 7776 称为“DTE 数据链路层规程”。它与 CCITXX. 25LAB“平衡型链路访问规程”兼容。

4）LAN 驱动程序和访问方式。

5）快速分组广域网，例如帧中继和异步传输模式（ATM）。

6）Microsoft 的网络驱动程序接口规范（NDIS）。

7）Novell 的开放数据链路接口（ODI）。

常用的链路常用产品主要有网卡、网桥和交换机等。

3. 网络层（Network Layer）

网络层建立在数据链路层之上，主要功能就是寻址，选择合适的路由（传输路径），使发送站点的数据能够正确无误地按照地址找到目的站点，并交付给目的站。

之所以要处理路由是因为在网络中，通信双方可能不在同一个网络，或不在两个邻接的网络。可能要经过许多个不同网络的站点和链路才能建立网络通信通道。这样，当一个数据从发送端发送到接收端接收，就可能要经过多个其他网络站点。这些站点只是先暂时存储

“路过”的数据，然后根据网络的状况选择下一个站点，再将数据分组发给它，直到把数据发送到接收方为止。

如果仅仅是单一网络，没有网络互连，这一层可以没有。

网络层的常用标准主要有：

1）ISO. DIS8208，称为“DTE 用的 X. 25 分组级协议”。

2）ISO. DIS8348 称为“CO 网络服务定义”（面向连接）。

3）ISO. DIS8349 称为“CL 网络服务定义”（面向无连接）。

4）ISO. DIS8473 称为“CL 网络协议”。

5）ISO. DIS8348，称为“网络层寻址”。

6）因特网协议（IP）。

7）Novell 的网间分组交换（IPX）。

8）Banyan 的 VINES 网间互联协议（VIP）。

此外还有一些标准大多只是规定网络层的部分功能。因此往往要在网络层同时使用几个标准，并根据网络的不同而作不同的组合。

网络层的常用硬件设备主要有网关和路由器。

物理层、数据链路层及网络层主要功能是处理数据通信。它们三者合称为 OSI 模型的通信子网。

4. 传输层（Transfer Layer）

这一层有几个译名，如传送层、运输层或转送层。信息的传送单位是报文。当报文较长时，先要把它分割成好几个分组，然后交给下一层（网络层）进行传输。

传输层的功能是在网络层及以下各层提供的网络通信通道上，根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式，向用户提供可靠的端到端（End-to-End）数据传输服务。它要确保数据传输无差错、不丢失或重复，并能按次序传输。

它屏蔽了会话层，使它看不见运输层以下的数据通信的细节。在通信子网中没有运输层。运输层只能存在于端系统（即主机）之中。运输层以上的各层就不再管信息传输的问题了。正因为如此，运输层就成为计算机、PLC 网络体系结构中最为关键的一层。

典型传输层常见的标准有 TCP 协议（即 ISO 8072），也称为“面向连接的传输服务定义”及 UDP 协议（即 ISO 8072），也称为“面向连接的传输协议规范”。

5. 会话层（Session Layer）

这一层也称为会晤层或对话层。在会话层及以上的更高层次中，数据传送的单位没有另外再取名字，一般都可称为报文。

会话层的主要功能是协调、同步对话。包括会话的初始化、执行及终止。

它虽然不参与具体的数据传输，但它却对数据传输进行管理。会话层在两个互相通信的应用进程之间，建立、组织和协调其交互（Interaction）。例如，确定是双工工作（每一方同时发送和接收），还是半双工工作（每一方交替发送和接收）。当发生意外时（如已建立的连接突然断了），要确定在重新恢复会话时应从何处开始。

会话层常见的标准主要有 DIS8236（会话服务定义）和 DIS8237（会话协议规范）等。

6. 表示层（Presentation Layer）

表示层要处理通信信息的表示问题，要为异种机通信提供一种公共语言，以便能进行互

操作。因为不同的计算机体系结构使用的数据表示法不同。例如，IBM 主机使用 EBCDIC 编码，而大部分 PC 使用的是 ASCII 码。在这种情况下，便需要会话层来完成这种转换。具体讲表示层的主要功能为数据翻译；编码和字符集转换；格式化；修改数据的格式；语法选择；对所用变换的初始选择和随后修改。如果需要，还要负责数据的加密、解密，数据的压缩与恢复。

对于数据，可以从两个侧面分析，一个是数据含义，即语义，另一个是数据的表示形式，即语法。像文字、图形、声音、文种、压缩、加密等都属于语法范畴。表示层设计了 3 类 15 种功能单位，其中上下文管理功能单位的作用就是沟通用户间的数据编码规则，以便双方有一致的数据形式，能够互相认识。ISO 表示层为服务、协议、文本通信符制定了 DP8822，DP8823，DIS6937/2 等一系列标准。

7. 应用层（Application Layer）

应用层是 OSI 参考模型中的最高层，直接为应用进程提供服务。其作用是负责用户信息的语义表示，并在两个通信者之间进行语义匹配，进行一些语义上有意义的信息交换。它要在实现多个系统应用进程相互通信的同时，完成一系列业务处理所需的服务。其服务元素分为两类：公共应用服务元素 CASE 和特定应用服务元素 SASE。

CASE 提供最基本的服务，它成为应用层中任何用户和任何服务元素的用户，主要为应用进程通信和分布系统实现提供基本的控制机制。

特定服务 SASE 则要满足一些特定服务，如文件传送，访问管理，作业传送，银行事务，订单输入等。这些将涉及虚拟终端，作业传送与操作，文件传送及访问管理，远程数据库访问，图形核心系统，开放系统互连管理等。

应用层的常用的标准主要有：

1）DP8649，公用应用服务元素。

2）DP8650，公用应用服务元素用协议，文件传送、访问和管理服务协议。

3）虚拟终止。

4）文件传输访问和管理（FTAM）。

5）分布式事务处理（DTP）。

6）信报处理系统（X. 400）。

7）目录服务（X. 500）。

这 7 层只是功能的划分，除物理层之外，不同站点的对等层之间没有物理联系，只是虚拟通信。该模型通信示意图如图 1-30 所示，其中虚线表示站点间虚拟通信。在同层间，虽然可进行信息交换，但只能是间接的。只有物理层才存在实际的通信。

在模型中，通信双方对等层之间交换数据的单元称协议数据单元（Protocol Data Unit，PDU）。其中，每个层都要依靠它的下一层提供的服务。为此，下层都是把上层的 PDU 划小（必要时），并加上头部（和尾部）进行封装。加上头部的目的是增加数据传输所需要的信息。所以，发送数据，数据自上向下传递的过程，实际就是不断封装的过程。而到达对方后，数据从下向上传递，则是不断拆封、组合的过程。

图 1-31 所示为源计算机 A 的应用层把信件 MA7 传输给目标计算机 B 的具体过程。它首先通过层间接口传给表示层。表示层对 MA7 作处理后，得到新信件 MA6，再送会话层，逐层下传，每层都进行相应操作，生成新的 PDU。

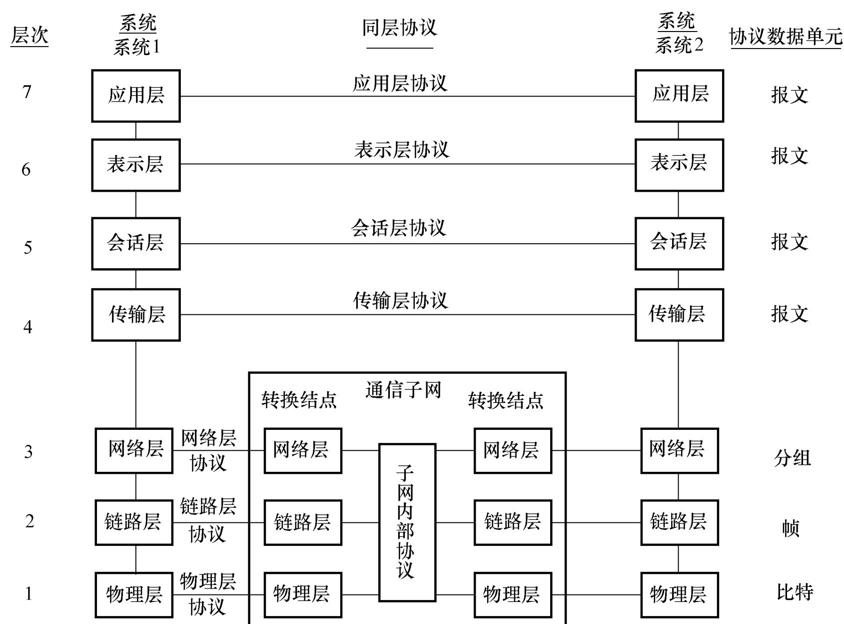


图 1-30　OSI 参考模型示意

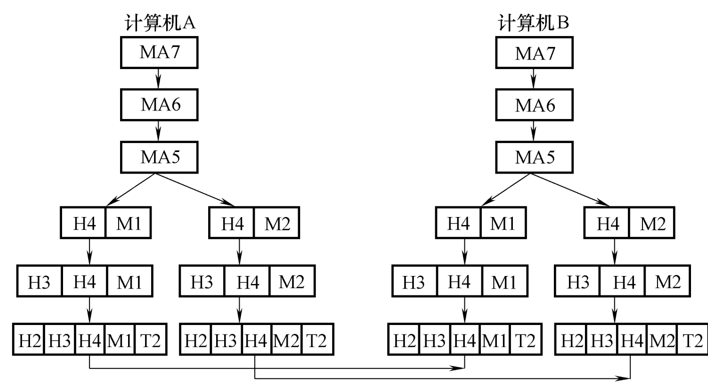


图 1-31　ISO 推荐模型通信实际过程

从图知，高层的信息单元少，而越下层越多，但每单个的 PDU 的信息容量少了。这主要是受信息缓冲器容量的限制及考虑到网络的效率。如图所示，在传输层，它把 MA5 分成 M1、M2 两个单元。传输层的信息单元称包（Packet）。在网络层，再加上本层的控制信号 H3 后再传给链路层。链路层的信息单元称为帧（Frame），容量更小。到了物理层才把一帧帧的信息按位传给计算机 B。

在计算机 B，其过程正好与计算机 A 相反。

如果在相同的层间进行虚拟通信，其过程也类似。只是不从最高层开始，而是从该层开始。有了这 7 层，并按此作软、硬件配置，不同厂家的计算机、PLC 等实现连网就有可能了。

为了对 OSI 有更简明的理解，表 1-9 给出了两个主机用户 A 与 B 对应各层之间的通信联系以及各层操作的简单含义。

表 1-9　主机间通信以及各层操作的简单含义

主机 H_A	控制类型	对等层协议规定的通信联系	简单含义	数据单位	主机 H_B
应用层	进程控制和用户进程	用户进程之间的用户信息交换	做什么	用户数据	应用层
表示层	表示控制	用户数据可以编辑、交换、扩展、加密、压缩或重组为会话信息	对方看起来像什么	会话报文	表示层
会话层	会话控制	建议和撤出会话，如会话失败应有秩序的恢复或关闭	轮到谁讲话和从何处讲	会话报文	会话层
传输层	传输端-端控制	会话信息经过传输系统发送，保持会话信息的完整	对方在何处	会话报文	传输层
网络层	网络控制	通过逻辑链路发送报文组，会话信息可以分为几个分组发送	走哪条路可到达该处	分组	网络层
数据链路层	链路控制	在物理链路上发送帧及应答	每一步应该怎样走	帧	数据链路层
物理层	物理控制	建立物理线路，以便在线路上发送位	对上一层的每一步怎样利用物理媒体	位（比特）	物理层

这 7 层模型虽较完善，但比较复杂。所以，至今只是参考，还没有一个实际网络完全按这个模型构建。

1.3.2　TCP/IP 模型与相应协议

TCP/IP（Transmission Control Protocol/Internet Protocol）为网络的传输控制协议/网际协议，源于美国国防部研究性网络 ARPANET。用它可将不同的网络实现无缝连接。它既是一个完整的协议簇，又是一个网络体系结构。它出现在 OSI/RM 模型之前，早已成为计算机网络事实上的标准，网络体系结构事实上的参考模型。当今互联网使用的都是这个模型与协议簇。

TCP/IP 网络体系结构分为 4 个层次，自下向上依次为网络接口层、网际层、传输层和应用层。在各个层都定义相应协议。

在 TCP/IP 参考模型中，去掉了 OSI 参考模型中的会话层和表示层（这两层的功能被合并到应用层实现）。同时将 OSI 参考模型中的数据链路层和物理层合并为主机到网络层。下面分别介绍各层的主要功能。

1. 网络接口层

这个层大体与 OSI 的物理层及数据链路层相当。是 TCP/IP 模型的最低层。但 TCP/IP 模型没有具体定义它的内涵。只是指出主机必须使用某种协议与互连网络连接，以便能在其上传递 IP 分组。这里没有具体的协议，为的是保证通过 TCP/IP 参考模型可将不同的物理网络互连起来。

2. 互连网（IP）层

互连网层也称网际层，负责源站点与目标站点之间的数据传输，相当于 OSI 参考模型中的网络层。

TCP/IP 是为包容各种物理网络技术而设计的，这种包容性主要体现在 IP 层中。在实际网络中，帧或报文格式、地址格式差别很大。TCP/IP 的重要思想之一就是通过 IP 将各种底层网络统一起来，达到屏蔽底层细节，提供统一界面的目的。

IP 向上层（主要是 TCP 层）提供统一的 IP 报文，使得各种网络帧或报文格式的差异性对高层已不复存在。IP 层是 TCP/IP 实现异构网络互连的最关键一层。

IP 层使用的 IP 协议主要用于负责 IP 寻址、路由选择和 IP 数据包的分割和组装。目前，常用的 IP 协议是 IP 协议的第四版本，即 IPv4，是互联网中最基础的协议，最多可支持 4294967296（2^{32}）个地址连接到 Internet。

3. 传输层

它与 OSI 参考模型中传输层的功能是一样的，即在源站点和目的站点的两个进程实体之间提供可靠的端到端的数据传输。

TCP/IP 模型提供了两个传输层协议：传输控制协议 TCP 和用户数据报协议 UDP。

TCP 协议是一个可靠的面向连接的传输层协议，它将某站点的数据以字节流形式无差错投递到互联网的任何一台机器上。发送方的 TCP 将用户交来的字节流划分成独立的报文，交给互连网层，并由其发送，而接收方的 TCP 将接收的报文重新装配，再交给接收用户。TCP 同时处理有关流量控制的问题，以防止快速的发送方淹没慢速的接收方。

用户数据报协议 UDP 是一个不可靠的、无连接的传输层协议，UDP 协议将可靠性问题交给应用程序解决。UDP 协议主要面向请求/应答式的交易型应用，一次交易往往只有一来一回两次报文交换，假如为此而建立连接和撤销连接，开销是相当大的。这种情况下使用 UDP 就非常有效。另外，UDP 协议也应用于那些对可靠性要求不高，但要求网络的延迟较小的场合，如话音和视频数据的传送。

4. 应用层

与 OSI 模型的 3 个高层相当。包括所有的高层协议。有远程登录协议（Telnet）、文件传输协议（File Transfer Protocol，FTP）、简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）、主机名字地址映射成网络地址的域名服务协议（Domain Name Service，DNS）、传输网络新闻协议（Network News Transfer Protocol，NNTP）和用于从 WWW 网上读取页面信息的超文本传输协议（Hyper Text Transfer Protocol，HTTP）协议等。

<table>
<tr><td>应用层</td><td colspan="4">FTP、TELNET、HTTP</td><td>SNMP、TFTP、NTP</td></tr>
<tr><td>传输层</td><td colspan="4">TCP</td><td>UDP</td></tr>
<tr><td>网络互连层</td><td colspan="5">IP</td></tr>
<tr><td rowspan="2">主机到网络层</td><td rowspan="2">以太网</td><td rowspan="2">令牌环网</td><td>802.2</td><td colspan="2">HDLC、PPP、FRAME-RELAY</td></tr>
<tr><td>802.3</td><td colspan="2">ELA/TIA_232，449、V35，V21</td></tr>
</table>

图 1-32　TCP/IP 模型各层使用的主要协议

图 1-32 所示为 TCP/IP 模型各层所使用的主要协议。

从图知，网络接口层除了支持以太网协议，还支持其他一些网络协议。

TCP/IP 协议使用一组由十进制数组成的 4 段数字（最大为 255）来确定计算机的地址。每段数字之间用小数点隔开，例如 122. 68. 73. 1，习惯上把这种识别计算机的数字称为 IP 地址。通过 IP 地址，操作系统可以方便地在网络中识别不同的计算机，在 TCP/IP 协议中提供了称为域名解析服务（DNS）的方案，它可以将 IP 地址转化为用文字表示的计算机名称，

例如 www. microsoft. com，这种用文字表示主机的方法，可以使用户更加容易理解 IP 地址所代表的含义或者拥有该地址的计算机所代表的公司或提供服务的领域，避免了纯数字的枯燥乏味。另外，TCP/IP 协议是一种可以路由的协议，通过识别子网掩码，可以在多个网络间传递和复制信息。

微软的联网方案也使用了 TCP/IP 协议，在 Windows2000Server 中，TCP/IP 协议与 DNS 以及动态主机配置协议（DHCP）配合使用。DHCP 用来分配 IP 地址，当用户计算机登录网络时，会自动寻找网络中的 DHCP 服务器，以便从 DHCP 服务器获得网络连接的动态配置，并获得 IP 地址。

TCP/IP 还有一个基本思想：任何一个能传输数据分组的通信系统，均可被看做是一个独立的物理网络，这些通信系统均得到平等对待。大到广域网、小到局域网，甚至两台机器之间的点到点专线以及拨号电话线路都被当做网络，这就是互联网的网络对等性。

TCP/IP 还具有以下特点：

1）TCP/IP 通信协议简单、灵活、易于实现，充分考虑不同用户的需求，并已经在现实的网络中使用。

2）TCP/IP 不是某特定厂商所制定的通信协议，是开放的协议标准，可以免费使用，并有组织负责管理，如统一的网络地址分配，整个 TCP/IP 设备在网中都具有唯一的地址等。

3）独立于特定的网络硬件与操作系统，可以运行在局域网、广域网，更适用于互联网中。

4）已经有相当数量的软件及操作系统采用 TCP/IP 通信协议作为建立网络的基础，而且相关的文件数量相当多，影响力大。

5）标准化的高层协议，可以提供多种可靠的用户服务。

正是这样，在 PLC 信息网中也有 TCP/IP 的应用。但 TCP/IP 也有不足，主要是没有明显地区分出协议、接口和服务的概念；不通用，只能描述它本身；主机-网络层只是个接口；不区分物理层和数据链路层。

1.3.3 企业网络模型

作为 PLC 参与的企业网络，大多不是一种网络，而是多种网络。所以，除了上述网络的层次结构模型，还有多种企业网络相互关系的模型。它描述的不是网络的不同层次结构，而是网络功能的级（层）次结构。与网络的层次结构一样，它也有标准组织推荐的模型，也有大 PLC 厂家推出的事实模型。

1. 企业网络标准模型

美国国家标准局曾为工厂计算机控制系统提出过一个如图 1-33 中所示的 NBS（National Bureau of Standards）企业网络模型。它建议企业建立 6 种网络，分为 6 级。并规定了每一级应当实现的功能，这一模型获得了国际广泛的承认。

Corporate	公司级
Plant	工厂级
Area	区间级
Cell/Supervisory	单元/监控级
Equipment	设备级
Device	装置级

图 1-33 NBS 企业网络模型

国际标准化组织（ISO）对企业网络的建模也进行了一系列研究，提出了一个如图 1-34 所示的 6 级（层）模型。尽管它与 NBS 模型各级内涵，特别是高层内涵有所差别，但两者在本质上是相同的。它的高 3 级（层）负责经营管

理，低 3 级（层）负责生产控制与过程监控。

2. 企业网络事实模型

多数 PLC 生产厂家也结合自身的 PLC 及其网络产品推出了企业网络。由于得到广泛应用，已成了事实模型。常用的模型多是金字塔 PP（Productivity Pyramid）结构。如图 1-35 所示为美国 AB 公司和德国 SIEMENS 公司的金字塔模型。尽管这些金字塔结构级（层）数不同，各级（层）的功能有所差异，但它们都表明 PLC 及其网络在工厂自动化系统中，由上到下，在各级（层）都发挥着作用。这些金字塔结构的共同特点是：上级（层）负责生产管理，下级（层）负责现场控制与检测，中间级（层）负责生产过程的监控及优化。

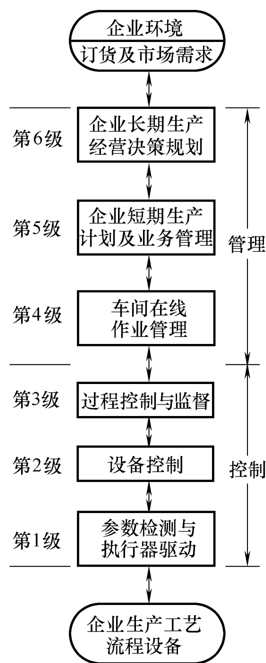


图 1-34　ISO 企业网络模型

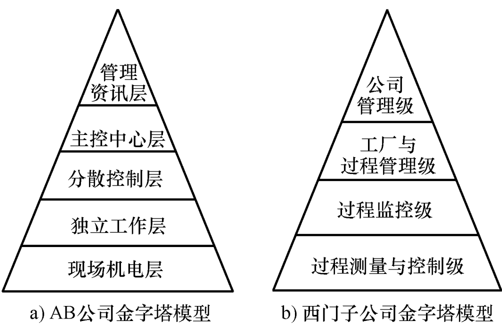


图 1-35　金字塔级（层）结构模型

1.4　计算机局部网络与 PLC 网络协议标准

关键词：IEEE802.3、IEEE802.4、IEEE802.5、标准、协议、PLC 网络协议、PLC 网络行业标准、PLC 网络事实标准

根据网络结构模型建立的各层具体协议，当然是由网络的设计与推出者制定的。但为了使所制定的协议便于执行，最好有标准可依。为此，相关国际组织已陆续制定有一系列协议标准。所以要了解协议，应首先对这些标准有所了解。

1.4.1　计算机局部网络标准

ISO 的 OSI/RM 是以广域网（WAN）为基础制定的，不够全面。局域网（LAN），特别 PLC 网络多采用共享通信介质的拓扑结构，若多个站点同时发送数据，就会出现冲突，而 OSI/RM 却对此没有解决方案。

为此，IEEE在1980年2月成立了局域网标准化委员会，对OSI/RM模型进行了改造，制定了一系列的标准，使其完善。这一系列标准称为IEEE802标准。该标准已被国际标准化组织（ISO）采纳、作为局域网的国际标准，称为ISO 802标准。在此标准中，LLC子层中规定了无确认无连接、有确认无连接和面向连接3种类型的链路服务。各个子标准之间的关系如图1-36所示。

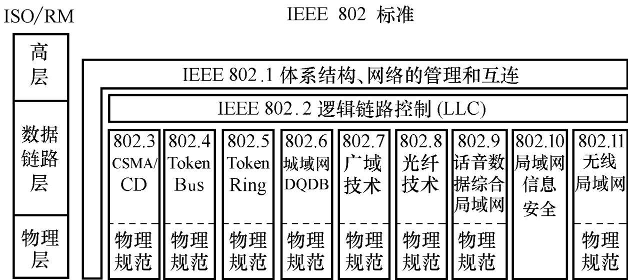


图1-36　IEEE 802标准系列

以下分别对这几个标准作简要介绍：

1. IEEE 802.1

它定义了IEEE 802标准和ISO开放系统互连（OSI）参考模型之间的关系。例如这个委员会为所有的802标准定义了48位的LAN站地址，这样每一个适配器就有唯一地址。IEEE把地址开始的3个字节赋予每一个供应商。然后每一个供应商负责为他的每个产品建立一个唯一的地址。

2. IEEE 802.2

它定义了逻辑链路控制（LLC）协议。这些协议确保数据在一条通信链路上可靠地传输。OSI协议栈中的数据链路层被分成了介质访问控制（MAC）子层和LLC子层。

LLC协议是由高级数据链路控制（HDLC）协议派生而来的，并且两者在操作上类似。注意，LLC提供了服务访问点（SAP）地址，而MAC子层提供了一个设备的物理网络地址。SAP指定了运行于一台计算机或网络设备上的一个或多个应用进程地址。

LLC提供了以下服务：

1）面向连接的服务。在这个服务中，一个会话是和一个目的站建立的，并且当数据传输结束时，就关闭这个会话。每个站点都自动地参与数据传输，但是这样的会话要求一个建立时间以及会话双方由于监控带来的额外开销。

2）应答式面向连接服务。在这种服务中，分组传输是需要应答的。

3）非应答式无连接服务。在这种服务中不用建立会话，分组只是发往目的地。高层协议负责请求重发丢失的分组。由于LAN的高可靠性，这种服务因此成为LAN上的通常服务。LLC帧格式及其控制字段定义如图1-37所示。

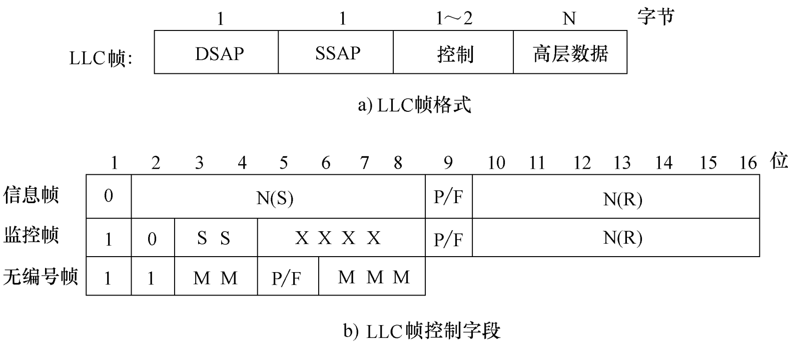


图1-37　LLC帧格式及其控制字段

LLC 帧分为信息帧、监控帧和无编号帧 3 类。信息帧主要用于信息数据传输。监控帧主要用于流量控制。无编号帧用于在 LLC 子层传输控制信号，以对逻辑链路进行建立与释放。LLC 帧的类型取决于控制字段的第 1、2 位，信息帧和监控帧的控制字段均为 2 字节长，无编号帧的控制字段为 1 字节。监控帧控制字段中的第 5 ~ 8 位为保留位，一般设置为 0。控制字段中的其他位的含义与 EELC 控制字段中的含义相同。

3. IEEE802.3（ISO 802.3）

它定义了争抢式总线网络，其基础是 XEROX 公司研制的以太网（Ethernet）。所定义的体系结构包括 MAC 子层和物理层。物理层又分为物理信令 PLS 和物理媒体连接件 PMA 两个子层。其体系结构示意图如图 1-38 所示。

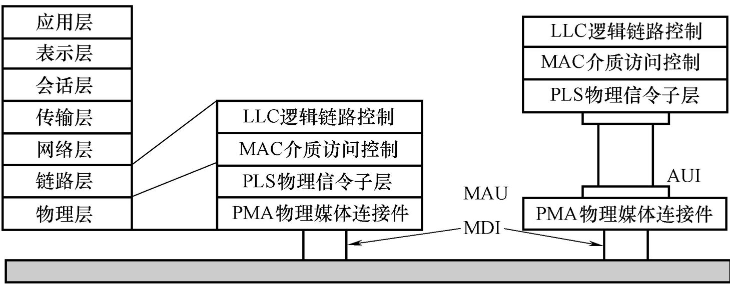


图 1-38　10Mbit/s 以太网体系结构

PLS 子层向 MAC 子层提供服务，它规定了 MAC 子层与物理层的界面，是与传输媒体无关的物理层规范。在发送比特流时，PLS 子层负责对比特流进行曼彻斯特编码。在接收时，负责对曼彻斯特解码。另外，PLS 子层还负责完成载波监听功能。PMA 子层向 PLS 子层提供服务，它负责向媒体上发送比特信号和从媒体上接收比特信号，并完成冲突检测功能。IEEE802.3 标准规定，PLS 子层和 PMA 子层可以在，也可以不在同一个设备中实现。比如标准以太网 10Base-5 是在网卡中实现 PLS 功能，在外部接收器中实现 PMA 功能的。所以在 10Base-5 以太网中，需要使用收发器电缆将外部收发器和网络站点连接起来，于是出现了两种 IEEE802.3 体系结构。

MAC 子层的核心协议是 CSMA/CD，它的帧结构如图 1-39 所示。

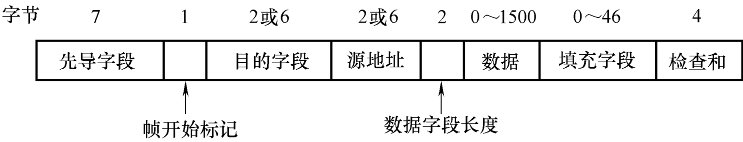


图 1-39　IEEE802.3 帧结构

其中，7 个字节的先导字段是接收方与发送方时钟同步用的，它的每个字节的内容都是 10101010。一个字节的帧开始标志，表示一个帧的开始，内容为 10101011。随后是两个地址段：源地址和目的地址，目的地址可以是单个的物理地址，也可以是一组地址（多点广播），当地址的最高位为 0 时，是普通地址，为 1 时，是组地址。2 字节的数据字段长度标志，指明数据段中的字节数。数据字段就是 LLC 数据帧，如果帧的数据部分少于 46 字节，

则用填充字段，使之达到要求的最短长度，其原因见后续叙述。

在 IEEE 802.3 标准中，定义目的地址和源地址长度是 2 字节或者 6 字节。因此帧的长度范围是 64 ~ 1518 个字节。需要注意的是在实际应用中，目的地址和源地址长度都是 6 字节，因此帧的实际最小长度为 72 字节。

IEEE802.3 支持的物理层介质和配置方式有多种，是由一组协议组成的。每一种实现方案都有一个名称代号，由以下 3 部分组成：

<数据传输率(Mbit/s)> <信号方式> <最大段长度(百米)或介质类型>

如 10BASE-5、10BASE-2、100BASE-T 等。这里，最前面的数字指传输速率，如 10 为 10Mbit/s，100 为 100Mbit/s。中间的 BASE 指基带传输，BROAD 指宽带传输。最后若是数字的话，表示最大传输距离，如 5 是指最大传输距离 500m，2 指最大传输距离 200m。若是字母则第一个表示介质类型，如 T 表示采用双绞线，F 表示采用光纤介质，第二个字母表示工作方式，如 X 表示全双工方式工作。

IEEE802.3 定义的争抢式总线含义是，多个站点连接在一根总线上，共享广播式的传输总线。每个站都是平等的采用竞争方式争得数据发送权。取得发送权的站点可向所有站点广播发送数据（报文）。当某个站识别到报文上的接收站名与本站的站名相同时，便将报文接收下来，否则不予处理。但由于这里没有专门的控制站，两个或多个站可能因同时发送数据而发生冲突，会造成报文作废，因此必须采取措施来防止冲突。

为此，简单的办法是，发送站在发送报文之前，先监听一下总线是否空闲，如果空闲，则发送报文，称之为“先听后讲”。但是这样做仍然有发生冲突的可能，因为报文在总线上传输到所有站点需一段时间，在这一段时间内，另一个站通过监听也可能会认为总线空闲而也发送报文，这样就会因两站同时发送而发生冲突。

为了防止这样的冲突，采取的措施是，发送报文开始的一段时间，仍然监听总线，采用边发送边接收的办法，把接收到的信息和自己发送的信息相比较，若相同，则继续发送，称之为“边听边讲”；若不相同，则说明有冲突，应立即停止发送，并发送一段简短的冲突标志（Jam），以表明总线不能再使用。通常把这种“先听后讲”和“边听边讲”相结合的方法称为 CSMA/CD（Carrier-Sense Multiple Access with Collision Detection）。

尽管有了这个“听”的检测，但如果有多个站点一检测到总线空闲，就都立即发送，肯定又都会检测到冲突，又都退出。进而，又是重复上述过程。这样长此下去的结果是，哪个站点也发送不了数据。所以，不能检测到总线空闲，就立即发送数据，而是要有退避机制，即检测到空闲时，都要随机延时一段时间后再发送。图 1-40 显示了采用 CSMA/CD 方法的流程图。

这个随机时间计算可用不同的算法。常用是称为二进制数退避算法（Binary Exponential Back off）。其工作原理如下：

- 如果一个站点发生了第一次冲突，就等待 0 或 1 个时隙（随机选择），然后重试。
- 如果它发生了第二次冲突，就等待 0、1、2 或 3 个时隙（仍是随机选择）。
- 在第三次冲突后，等待时间从 0 ~ 7 个时隙不等。
- 一般来说，在第 n 次冲突以后，如果 $n \leqslant 10$，等待时间从 $0 \sim 2^{n-1}$ 个时隙。如果 $n > 10$，等待时间从 0 ~ 1024 个时隙。
- 在发生第 16 次冲突以后放弃。这时网络可能出了问题，要人工诊断解决。

很明显，这种方法试图通过控制可能的时隙数来使过长的等待减到最小。毕竟，如果两个站点冲突了，它们有 50% 的机会在第二次尝试中获得成功（假设没有别的站点要发送数据）。但如果有很多个站点发生了冲突，即使是仅有一个站点在第二次尝试中成功的机会也是很小的。成功的站点必须选择 0 或 1 个时隙，而其他的所有站点选剩下的另一个。通过在每次冲突后增加可能的时隙数，再次冲突的机会将按指数规律下降。只有当前面所有的尝试都失败了以后，才有可能出现大的时隙数。这时，让某些站点长时间地等待也许是唯一的解决方案。

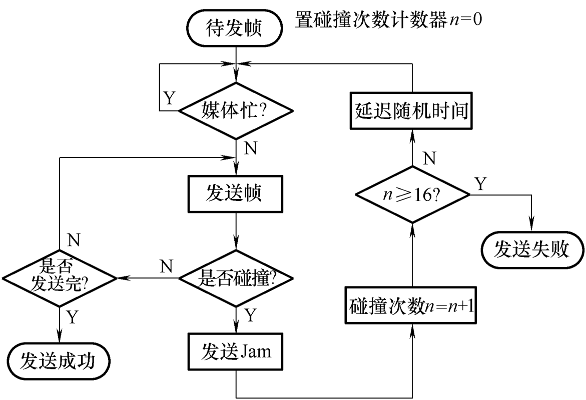


图 1-40　CSMA/CD 流程图

此外，如何保证“边听边讲”是否有效也是要考虑的。如果发送帧（报文）太小，到发送完毕虽没能检测到冲突，但也不能确认发送的帧没有冲突。因为有这样可能，信号传播的前端快到，但还没有到最远的目的站，对方由于没有检测到这个信号，而发送自己的帧，结果这两个帧产生冲突，而这个冲突信号返回到发送站点还要时间，但如果发送帧太小，这时此帧已发送完毕，就没能检测到这个冲突。

当然，帧的最大长度也要有所限制。这可使其他站点也能得到发送权，以确保使网络正常工作。对于 10Mbit/s 的基带 CSMA/CD 网，MAC 帧的总长度为 64 ~ 1518B。如果帧太长，可进行分组；而帧太短，则须填充字段必要的字节。

CSMA/CD 这种争用协议最大的优点是算法较简单，技术上易实现。每一站点处于平等地位，无需知道其他站点的细节。站点添加与站点退出对网络都无关紧要。所以，得到了越来越广泛的应用与快速的发展。很适用于办公自动化等对数据传输实时性要求不严格和通信负荷较轻的应用环境中。

4. IEEE802. 4

它定义了令牌总线网络。是由 GM 公司支持的制造自动化协议（Manufacturing Automation Protocol，MAP）派生而来的。从物理上看，它属于一种总线结构的局域网，但从逻辑上看，它又属于一种环形结构的局域网。它用令牌（实际是一个带有地址字段的短帧）授予站点的数据发送权，只有获得令牌的站点才能发送数据。它的每一站点都设定有一个本身逻辑地址及上一个站点地址和下一个站点地址，如图 1-41 所示。

从图中可以看出，在物理结构上它是一个总线结构局域网，但是在逻辑结构上，又成了一种环形结构的局域网。如图所示，该网络共有 5 个站点，但只有 4 个加入逻辑环。令牌在逻辑环上依次（A→D→B→C→A）循环传递，与物理位置无关。

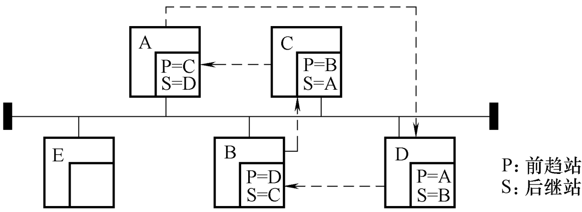


图 1-41　令牌总线网

在网络空闲时，从逻辑上看，令牌是按上述设定的顺序传递；而从物理上看，令牌广播到总线上的所有站点，只有站点地址和令牌帧的目的地址相符的站点才有权获得令牌。

获得令牌的站点，如果有数据要发送，则可立即传送数据，完成发送后再将令牌传送给下一个站点；如果没有数据要发送，则应立即将令牌传送给下一个站点。由于总线上传递令牌是按顺序依次进行的，因此所有站点都有数据发送权。

为了使站点等待令牌的时间确定，需要对每一站点发送数据帧的最大长度有所限制。如果所有站点都有数据发送，在最坏的情况下，则等待获得令牌的时间应该等于网络所有令牌传送时间和最大长度数据帧发送时间的总和。如果只有一个站点有数据要发送，在最坏的情况下，等待时间只是令牌传送时间的总和。上述两者情况，平均等待时间都是它的一半，而实际等待时间则是在这一区间范围内，比较确定。

令牌总线还提供了不同的优先级机制。优先级机制的功能是将待发送的帧分成不同的访问类别，赋予不同的优先级，并把网络带宽分配给优先级较高的帧，而当有足够的带宽时，才发送优先级较低的帧。令牌总线MAC帧格式如图1-42所示。

≥1	1	1	2或6	2或6	≥0	4	1 字节
前导码P	SD	FC	DA	SA	数据	FCS	ED

SD：起始定界　　FC：帧控制　　DA：目的地址

SA：源地址　　FCS：帧校验序列　　ED：结束定界符

图1-42　令牌总线MAC帧格式

帧校验序列FCS使用32位CRC码，校验范围为SD与ED之间的帧内容。数据字段有3类，即LLC协议数据单元，MAC管理数据和用于MAC控制帧的数据。在SD和ED之间的字节数应少于8191。另外还有异常终止序列格式，仅由SD和ED两个字节组成。

令牌总线的主要操作如下：

1）环初始化，即生成一个顺序访问的次序。网络开始启动时，或由于某种原因，在运行中所有站点不激活的时间超过规定的时间，都需要进行逻辑环的初始化。初始化的过程是一个争用的过程，争用结果只有一个站能取得令牌，其他的站点用站插入的算法插入。

2）令牌传递算法。逻辑环按递减的站地址次序组成，刚发完帧的站点将令牌传递给后继站，后继站应立即发送数据或令牌帧，原先释放令牌的站监听到总线上的信号，便可确认后继站已获得令牌。

3）站插入环算法。必须周期性地给未加入环的站点以机会，将它们插入到逻辑环的适当位置中。如果同时有几个站要插入时，可采用带有响应窗口的争用处理算法。

4）站退出环算法。可以通过将其前趋站和后继站连接到一起的办法，使不活动的站退出逻辑环，并修正逻辑环递减的站地址次序。

5）故障处理。网络可能出现错误，这包括令牌丢失引起断环，重复地址、产生多个令牌等。网络需对这些故障做出相应的处理。

令牌总线网络通过总线拓扑结构使用的是75Ω CATV同轴电缆构造。IEEE802.4标准的宽带特性，支持在不同的信道上同时进行传输。宽带电缆有较强的传输能力，传输率可达10Mbit/s。

令牌总线网络的令牌传递顺序不是根据站的物理位置确定，因此必须有一个有效的MAC子层协议来管理。从IEEE802.4标准的原文超过200页之多可看出，它的MAC子层协议多么复杂。所以，目前计算机网络已不用它了。但PLC网络由于通信的确定性要求很高，

所以还常用它。

5. IEEE802. 5

它定义了令牌环（TokenRing）网络。在物理上，令牌环网络是一个由一系列环接口和这些接口间的点到点链路构成的闭合环路。而各站点则通过环接口连接到网上。原来是由 IBM 公司于 20 世纪 70 年代开发的，现在也仍是 IBM 主要的局域网技术。而 IEEE802. 5 和 IBM 公司的令牌环网标准基本兼容。

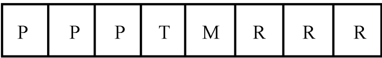
IEEE802. 5 令牌环的 MAC 帧有两种基本格式：令牌帧和数据帧。



SD：起始定界　　AC：访问控制　　FC：帧控制　　DA：目的地址
SA：源地址　　FCS：帧校验序列　　ED：结束定界符　　FS：帧状态

令牌帧只有 3 个字节长，数据帧则可能很长。这两种帧都有一对起始定界符 SD 和结束定界符 ED 用于确定帧的边界。

访问控制字段 AC 的格式如下：

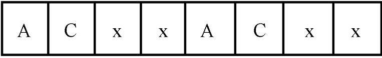


其中 T 为令牌/数据帧标志位，为“0”表示令牌，为“1”表示数据帧。M 为监控位，用于检测环路上是否存在持续循环的数据帧。PPP（3bit）为优先级编码，RRR（3bit）为预约编码。

帧控制字段 FC 中的前两位标志帧的类型。“01”表示一般信息帧，即其中的数据字段为上层提交的 LLC 帧；“00”表示 MAC 控制帧，此时其后的 6 位用以区分控制帧的类型。信息帧只发送给地址字段所指的目的站点，控制帧则发送给所有站点。控制帧中不含数据字段。

数据字段的长度没有下限，但其上限受站点令牌持有时间的限制。

帧状态字段 FS 的格式如下：



字段中设置了两位 A 和两位 C，其中 4 位未定义。A 为地址识别位，发送站发送数据帧时将该位置“0”，接收站确认目的地址与本站相符后将该位置“1”。C 为帧复制位，发送站发送数据帧时将该位置“0”，接收站接收数据帧后将该位置“1”。重复的 A、C 是为了提高可靠性。

结束定界符 ED 除了用于指示帧的结束边界外，其最后一位还用做差错位，发送站发送数据帧时将该位置“0”。任何一个站点转发该数据帧时发现有错，都可以将该位置“1”。

令牌环网的工作过程为

1）网络空闲时，只有一个空闲令牌（帧）在环路上绕行。

2）当一个站点要发送数据时，必须获得一个空闲令牌。获得后先将令牌的相应标志位置为“1”，随后发送置“1”后的令牌（帧）及数据（帧）。

3）环路中的每个站点边转发数据，边检查数据帧中的目的地址，若为本站点的地址，便读取其中所携带的数据。并对数据帧置上已读取标志及相关信息。

4）数据帧绕环一周返回时，发送站将其从环路上撤销。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧，否则释放缓冲区中的待确认帧。

5）发送站点完成数据发送后，重新产生一个空闲令牌传至下一个站点，为其他站点提供获得令牌的机会。

当令牌在环路上绕行时，可能会产生令牌的丢失，此时，应在环路中插入一个空令牌，以确保环路的利用率。而令牌的重复也会破坏网络的正常运行，也要将多余的予以撤销。为此，必须设置一个监控站点，以保证环路中只有一个令牌绕行。

令牌环的主要优点在于其访问方式具有可调整性和确定性，且每个站点具有同等的介质访问权。同时，还提供优先权服务，具有很强的适用性。同时，它发送的数据量较大，可达4500字节。它的主要缺点是要有监控站点，维护复杂，实现较困难。同时，在轻载时，网络利用率较低。

要强调的是，令牌环网的各站点不是收到全部数据后再转传，而是边收边传。这里就存在一个问题，是否发送站没有把发送帧全部发完，就有先发出去的位已返回？如真是这样当然是不允许了。但在实际上信号在网络上传播是有时延的。同时，每经过一个接口也都会有时延。只要这些延时足够长，足以把要发送帧全部发出去就没有问题了。

这里，这个延时用环路比特长度来表示。它反映环上可容纳的最大帧的长度。环路比特长度可由下式计算：

环路比特长度 = 信号传播时延 × 数据传输速率 + 接口延迟位数（接口的延时也折算为位）

= 环路媒体长度 × 5（μs/km）× 数据传输速率 + 接口延迟位数

式中，5μs/km即为信号传播速度200m/μs的倒数。

例如，某令牌环媒体长度为10km，数据传输速率为4Mbit/s，环路上共有50个站点，每个站点的接口引入1位延迟，则可计算得

环路比特长度 = 10km × 5μs/km × 4Mbit/s + 1bit × 50

= 250bit

说明这个环路最大可传送的帧为250bit。

如果由于环路媒体长度太短或站点数太少，以至于环路的比特长度不能满足数据帧长度的要求，可以在每个环接口引入额外的延迟，如使用移位寄存器等。以确保环路能容纳下最大的帧长度。

此外，光纤分布式数据接口（FDDI）也是基于802.5令牌环协议的，它是由Accredited标准委员会（ASC）X3T9开发的。FDDI数据传输速率达100Mbit/s，采用4B/5B编码，要求信道媒体的信号传输率达到125Mbaud。

光纤分布数据接口（FDDI）是目前成熟的LAN技术中传输速率最高的一种。使用光纤作为传输媒体具有以下优点：较长的传输距离，相邻站间的最大长度可达2km，最大站间距离为200km；具有较大的带宽，FDDI的设计带宽为100Mbit/s；具有对电磁和射频干扰抑制

能力，在传输过程中不受电磁和射频噪声的影响，也不影响其设备；光纤可防止传输过程中被分接偷听，也杜绝了辐射波的窃听，因而是最安全的传输媒体。

由光纤构成的 FDDI，其基本结构为双环的。一个环为主环，另一个环为备用环。当主环上的设备失效或光缆发生故障时，主环可向备用环切换，以维持 FDDI 的正常工作。这种故障容错能力是其他网络所没有的。

令牌环网络的令牌也比较复杂，目前计算机网络也已不用它了。但它的通信确定好，所以，有的 PLC 网络还用它，如 OMRON 的 SYSMAC NET 就采用这种方式。不过在 OMRON 新的机型中这个 SYSMAC NET 也已不用了。

6. IEEE802.6

城域网标准，定义了一个高速协议，协议规定网上的每个站点都使用一种叫分布式队列双总线（DQDB）的访问方法共享一条双光纤总线。双总线提供了容错特性，当总线发生故障时，它能保持连接的正常工作。MAN 标准是为一个大约 50km 的城域范围内提供数据、声音和视频服务而设计的，MAN 标准规定的数据传输率是 1.5Mbit/s、45Mbit/s 和 155Mbit/s。DQDB 是交换式多兆位数据服务（SMDS）的基本访问协议，SMDS 是许多公共电信局提供的一种在城域范围内建立专用网的方法。DQDB 是一个信元中继网，交换固定长度为 53 字节的信元；因此它与宽带 ISDN（B—ISDN）和异步传输模式（ATM）兼容。信元的交换发生 802.2 的逻辑链路控制层。

MAN 服务有无连接服务，面向连接服务和实时视频服务。总线上有许多定长槽，这些槽是放置那些在总线上传递的数据的。任何一个想传输的站点只需简单地把数据放在一个或多个槽中。但是，为了适应时间敏感的同步数据，固定间隔的定长槽必须保留以担保数据按时按序到达。

7. IEEE802.7

宽带技术咨询组。向其他分委员会提供有关宽带连网技术的技术咨询。

8. IEEE802.8

光纤技术咨询组。当用光纤来代替现有的基于铜缆的网络时，该组会向其他分委员会提供有关光纤网方面的技术咨询。

9. IEEE802.9

综合数据声音网 IEEE802.9 工作组。其工作是把声音、数据和视频信号集成到 802 局域网（LAN）和综合业务数字网（ISDN）上传输。规范中定义的站点包括电话、计算机和视频编码/解码器。该规范已经被称为综合的声音和数据规范，或 IVD。这项服务在使用铜质双绞线的两个站点之间的通道连接中提供能携带数据和声音信息的多路复用流。标准中定义了几种不同类型的通道，包括全双工 64Kbit/s 无交换、电路交换或分组交换通道。

10. IEEE802.10

网络安全技术咨询组。这个组的主要工作是定义在多个网络上进行互操作时的标准安全模型，在这个模型中加入鉴别和加密方法。

11. IEEE802.11

IEEE802.11 是第一代无线局域网标准之一。该标准定义了物理层和媒体访问控制（MAC）协议的规范，允许无线局域网及无线设备制造商在一定范围内建立互操作网络设备。与 802.3 相比，802.11 有如下新特点：在物理层定义了数据传输的信号特征和调制方

法，定义了两个射频（RF）传输方法和一个红外线传输方法。RF 传输标准是直接序列扩频（DSSS）和跳频扩频（FHSS）。由于在无线网络中冲突检测较困难，媒体访问控制（MAC）层采用避免冲突（CA）协议，而不是冲突检测（CD），具有独特的媒体访问控制机制，以 CSMA/CA 的方式共享无线媒体。

IEEE 802.11 是 1997 年制定的是原始标准（2Mbit/s，工作在 2.4GHz）。后续还有很多有关改进标准如：

IEEE 802.11a，1999 年，物理层补充（54Mbit/s，工作在 5GHz）。

IEEE 802.11b，1999 年，物理层补充（11Mbit/s，工作在 2.4GHz）。

IEEE 802.11c，符合 802.1D 的媒体接入控制　层桥接（MAC Layer Bridging）。

IEEE 802.11d，根据各国无线电规定做的调整。

IEEE 802.11e，对服务质量（Quality of Service，QoS）的支持。

IEEE 802.11g，2003 年，物理层补充（54Mbit/s，工作在 2.4GHz）。

IEEE 802.11h，2004 年，无线覆盖半径的调整，室内（indoor）和室外（outdoor）信道（5GHz 频段）。

IEEE 802.11i，2004 年，无线网络的安全方面的补充。

IEEE 802.11j，2004 年，根据日本规定做的升级。

IEEE 802.11m，维护标准；互斥及极限。

IEEE 802.11n，更高传输速率的改善，支持多输入多输出技术（Multi-Input Multi-Output，MIMO）。

IEEE 802.11k，该协议规范规定了无线局域网络频谱测量规范。该规范的制定体现了无线局域网络对频谱资源智能化使用的需求。

IEEE 802.11p，这个通信协定主要用在车用电子的无线通信上。它在设定上是从 IEEE 802.11 来扩充延伸，从而符合智能交通系统（Intelligent Transportation Systems，ITS）的相关应用。等等。

12. IEEE802.12

需求优先（100VG-AnyLAN）委员会。正用由惠普公司和其他供应商共同提出的需求优先访问方法来制定 100Mbit/s 的以太网标准。规定的电缆是 4 线铜质双绞线，需求优先访问方法是通过一台中心 Hub 来控制对电缆的访问。优先级方法可有效地支持实时多媒体信息的发送。

以上只是对 IEEE802 的一些标准做点儿简要说明。对 PLC，除 IEEE802.2 外，目前采用的主要标准是 IEEE802.3、IEEE802.4 及 IEEE802.5。

1.4.2　PLC 网络行业标准

PLC 网络也都是分层的。但是它的分层多把 ISO/RM 相邻几层的功能合并。目的是使网络简化，并具有适应性、可扩展性，用户可以根据投资情况及生产的发展，从单台 PLC 到网络，从底层向高层逐步扩展。

它的对应层也都有相关的协议，而这些协议也多是参考计算机网络的标准制定的。当然，如果不能满足要求，有的可能是全部或部分由自己定义。这个协议要处理的问题主要有：

1）通信环境约定，如电磁环境、通信距离等；

2）站点数量约定，如同一个网段的最多站点数，网络的最多站点数等；

3）网络拓扑约定，是星形、总线形，还是环形等；

4）站点数据交换约定，是点对点，还是点对多点等；

5）传输媒介冲突仲裁方式约定，是 CSMA/CD，还是令牌等；

6）传输数据量约定；

7）数据传输速率约定；

8）数据传输实时性约定；

9）CPU 处理能力约定。

PLC 厂家很多，同一厂家的 PLC 网络类型很多，协议也很多。网络类型与网络协议之多也是 PLC 网络的一大特点。网络不同、网络协议不同，如果没有像网桥、网关这样的站点或组件，就不能相互接入。

PLC 网络协议是与具体网络联系在一起的。什么样的 PLC 网络就有什么样的网络协议。反过来说也一样，什么样的网络协议，就有什么样的 PLC 网络。但是，网络与协议也不是一一对应的。一种网络可能要用到多种协议。反过来，一种协议也可用于多种网络。

以上两节介绍的模型及标准并不等于网络协议，它只是制定网络协议的参考。真正的 PLC 网络协议的制定及 PLC 网络的推出要由 PLC 厂家完成。

要指出的是，PLC 网络协议多是专用的。出自商业利益，相当多是不公开的。使用这样的协议，要用到厂家提供的工具软件。因此对这样的协议就不好深究了，着重点放在怎么用好它就够了。

然而随着 PLC 技术的进步，也出现了国际的 PLC 行业标准。其中也有关网络通信部分的推荐。只是这些标准多只是用作参考。以下将对其作简要介绍。

1. PLC 行业标准

PLC 行业标准为 IEC61131。其前身为（1998 年前）为 IEC1131。目前，不仅 PLC，而且 DCS、HMI 以及现场总线等制造商逐步提供基于此标准的产品。

IEC61131 标准将信息技术领域的一些先进的思想和技术（如软件工程、结构化编程、模块化编程、面向对象的思想，以及网络通信技术等）引入工业控制领域，弥补或克服了传统的 PLC、DCS 等控制系统的弱点（如开放性差、兼容性差、应用软件可维护性差以及可再用性差等）。对于符合这一标准的控制器，即使它们由不同制造商生产，其编程语言也是相同的，其使用方法也是类似的，因此工程师们可以做到“一次学习、到处使用”，从而减少了企业在人员培训、技术咨询、系统调试和软件维护等方面的成本。

IEC61131 国际标准包括 8 部分。Part1：综述；Part2：硬件；Part3：可编程语言；Part4：用户导则；Part5：通信；Part6：现场总线通信；Part7：模糊控制编程；Part8：编程语言的实施方针。IEC61131-3 是 IEC61131 中最重要、最具代表性的部分。IEC61131-3 国际标准将是下一代 PLC 的基础。IEC61131-5 是 IEC61131 的通信部分，通过 IEC61311-5，可实现可编程序控制器与其他工业控制系统、如机器人、数控系统、现场总线等的通信。

在 IEC61131 的各个部分陆续公布之后，我国的工业过程测量和控制标准化委员会按与 IEC 国际标准等效的原则，组织了该标准的翻译出版工作。于 1995 年 12 月 29 日以 GB/T 15969.1 ~4颁布了 PLC 的国家标准。该标准只涉及 IEC61131 的第一 ~ 四部分，没有

纳入1995年以后出版的第五部分通信、第七部分模糊控制编程软件工具、第八部分IEC61131—3语言的实现导则。

进入21世纪，国产PLC，如和利时LK、LM机，其编程语言也采用了IEC61131-3标准。若干新推出的DCS也公开宣称符合或兼容IEC61131-3标准。

2. PLC行业标准中通信部分

IEC61131-5为PLC通信部分标准。描述的是PLC的通信问题，即通过通信网络连接在一起的多台PLC之间如何实现状态及控制信息的交换、如何启动执行命令。执行命令包括重新启动资源和下载配置等。

（1）IEC61131-5的通信服务

包括两个方面：服务器设备和客户设备。

IEC61131-5以国际标准化组织（ISO）的网络的7层协议模型为基础，在第七层应用层之上建立了IEC61131-5的通信模型，所以，从理论上来说，IEC61131-5允许各PLC之间通过任何类型的网络进行通信。定义在IEC61131-5中的通信设备的许多概念来自IEC61131-3，如存取路径和通信功能块等。

通信功能块和相关的数据类型是用IEC61131-3中的概念和语言来定义的。IEC61131-5的通信模型如图1-43所示。

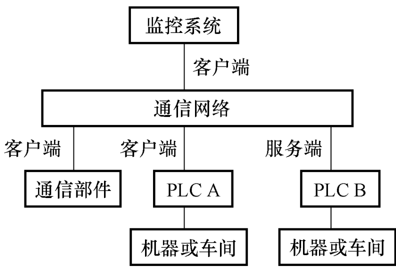


图1-43　IEC61131-5通信模型

一个PLC可以相当于一个服务器，为客户提供信息和对客户的请求做出反应，也可以相当于一台客户，向服务器请求信息和要求服务。其他的设备，诸如监控系统（Supervisory system）和其他非IEC61131-3相容设备也可以作服务器或客户。

通信协议（如以太网）允许非限定数量的PLC服务器和客户共存在同一个网络中。在许多情况下，一台PLC既可以作为一些PLC的服务器，又可以作为其他一些PLC的客户。

IEC61131-5标准仅仅定义了在PLC之内的通信设备，如PLC A和B的通信设备，并没有定义其他外部的客户的通信设备。

（2）IEC61131-5规定支持的应用功能

每一台PLC可提供通信设备，以支持下面的特殊应用功能：设备检验；数据获得；控制程序执行和I/O控制；应用程序传送；用户应用程序的同步；警告报告；连接管理。

（3）IEC61131-5规定的PLC主要子系统。

此子系统见表1-10。

对每一个子系统，其状态信息用一个标准格式的采用IEC61131-3中的数据类型表示的数据结构来描述。各个PLC子系统有相似的状态信息项。每一个子系统有一个称为“health（健康状况）”的初始化项，它有3个状态：GOOD、WARNING、BAD。每一个子系统的状态信息还包括特定的产品状态信息，诸如诊断错误、操作状态等。每一个子系统能够通过预定义的存取路径、直接地址，存取状态信息。IEC61131-5定义了一套复杂的保留直接地址用于存取PLC内的每一个子系统的状态。如%S0是主PLC状态的直接地址，%S3是第三子系统状态的直接地址。

（4）IEC61131-5 标准允许 PLC 之间交换信息和控制信号

表 1-11 列出了标准提供的通信设备和通信功能块。

表 1-10 PLC 主要子系统

序号	子系统
1	PLC 系统
2	I/O 子系统
3	处理器
4	电源单元子系统
5	内存子系统
6	通信接口
7	特殊功能子系统

表 1-11 PLC 通信设备和通信功能块

通信设备	通信功能块
连接管理	连接
部件确认	在状态、不在状态
数据访问	读、发送、接收
控制	写、发送、接收
报警	提示、报警
变量管理	远程变量

1）连接管理（Connection Management）。通信功能块通过通信通道读写远程 PLC。通信通道的建立是通过调用 CONNECT 功能块实例化，并将远程 PLC 的完全网络地址提供给 CONNECT 功能块来实现的。CONNECT 功能块返回一个本地通信通道的标识，所以，需要与特定的远程 PLC 通信的全部通信功能块能够使用该开放的通信通道。

2）设备确认（Device Verification）。STATUS 和 UNSTATUS 功能块读取远程 PLC 状态的设备。

3）数据获得（Data Acquisition）。数据获得关心的是从远程 PLC 读取变量值，读取变量值的方法有两种：

① 轮询（Polled）：READ 功能块能周期性地或在特定触发器条件下读取被选变量的值。

② 编程（Programmed）：远程 PLC 能够决定在何种条件下提供数据消息。远程 PLC 内的 USEND 功能块能够传送由 URCV 功能块接收的未经请求的数据。

4）控制（Control）。有两种方法用于实现本地控制软件和远程控制软件的交互：

① 参量法（Parametric）：该种方法允许本地 PLC 通过写值到关键变量，调整远程 PLC 的行为。使用 WRITE 功能块，允许将值写入到远程 PLC 内的被选的“存取路径（access-path）”变量中。

② 互锁法（Interlocked）：该种方法提供了一种控制事务处理的方法，即本地 PLC 请求远程 PLC 执行一个操作，接着返回操作完成的信号。这种事务处理是通过使用本地 PLC（客户）内的 SEND 的功能块和远程 PLC 内的 RCV 功能块来完成的。

5）报警报告（Alarmreport）。当某一预定的报警条件产生时，PLC 能向被选的远程 PLC 发出信号。远程 PLC 能够发送一个确认信号，返回给本地 PLC，告知报警报告已经收到了。ALARM 和 NOTIFY 功能块能够产生确认和非确认的报警报告。

6）变量范围管理（VariableS cope Management）。变量范围管理标识了各种各样的 IEC61131-3 语言或其他特定实现的名称范围。

（5）与 MMS 关系

IEC61131-5 考虑到了通信功能块映射到 ISO/IEC9605-5 的制造报文规范（Manufacturing Message Specification，MMS）中的给定服务的情况。MMS 特定于 MAP（Manufacturing Automation Protocol）的应用层。MAP 最初是由美国的通用公司在 1980 年推出的一种工业通信系统，MMS 标准定义了一系列服务，这些服务允许工业设备、单元控制器和监控系统通过一个通信网络交换信息。每一个服务特定为一个事务处理。一系列事先定义的数据项被传送给一个远程设备，接着就要求一系列事先定义的响应中的一个作出响应。请求信息和响应信息

具有足够的柔性来考虑附加的特定数据的实现。

定义在标准中的 MMS 映射包含了在表一中全部设备。每一个功能块使用一个已定义的 MMS 服务的子集。如 STATUS 功能块将使用 MMS 的“状态”服务。每一个功能块的实现将调用一系列定义的 MMS 服务。

这将允许与 IEC 相容的设备之间能够借助于任一基于 MMS 的网络进行互操作。采用 MMS 还能够使得基于 MMS 网络的不是采用 IEC61131-3 标准实现的设备与基于 IEC61131-3 标准的 PLC 进行通信。如一台在 MMS 网络上的数控机床（NC）能够对基于 IEC61131-3 标准的 PLC 内的 STATUS 功能块作出响应。

IEC61131-5 定义了 IEC61131-3 与 MMS 之间的映射以及相应的数据类型。IEC61131-5 还定义了数据类型的兼容性规则，还定义了 IEC61131-3 名称范围到各式各样的 MMS 域以及 MMS 事务处理的映射。

IEC61131-5 的通信模型的建立及其通信功能块到 ISO/IEC9605-5 的制造报文规范（Manufacturing Message Specification，MMS）中的给定服务的映射的建立，不但从理论上实现了各 PLC 之间通过任何类型的网络进行通信的能力，而且还大大地扩展了 PLC 系统与其他的自动化控制系统如数控机床（NC）、机器人等进行通信、集成的能力。IEC61131-5 标准很好地适应了自动化系统的未来发展对开放性提出的要求，这使得 IEC61131 可以很好地适应于 21 世纪。

1.4.3　PLC 网络事实标准

PLC 网络可参考的除了行业标准，更有力的标准还是一些大公司为主的协会开发的网络标准。由于这些标准有大公司的经验及相应的协会支持，同时，与现场总线的标准还有共通，而且随着网络技术的进步，还在不断地扩充、修改与完善。因而有相当大的生命力与覆盖面。也往往成为事实标准。这些标准及行业协会有：

1. DeviceNet 标准

DeviceNet 标准在 1994 年问世，由美国开发与生产 PLC 的著名厂家——Rockwell 公司开发，发展起来的一种基于 CAN（Controller Area Network）技术的开放型、符合全球工业标准的低成本、高性能的通信网络。于 1995 年，DeviceNet 成为国际标准 IEC62026-3《低压开关设备和控制设备控制器设备接口》，后又被列为欧洲标准，在北美及亚太地区都有日益广泛的应用，也是实际上的亚洲和美洲的 PLC 设备网标准。

DeviceNet 总线由 DeviceNet 总线的组织机构，即“开放式设备网络供货商协会”，简称 ODVA（Open DeviceNet Vender Association）负责推广。ODVA 是一个独立组织，管理 DeviceNet 技术规范，促进 DeviceNet 在全球的推广与应用。ODVA 实行会员制，会员分供货商会员（Vender Members）和分销商会员（Distributor Member）。ODVA 现有供货商会员 300 多个，其中包括 ABB、Rockwell、PhoenixContacts、OMRON、Hitachi、Cutler-Hammer 等几乎所有世界著名的电器和自动化元件生产商。

2002 年 10 月 8 日 DeviceNet 被批准为中国国家标准 GB/T18858.3—2002，并于 2003 年 4 月 1 日开始实施。标准名称为《低压开关设备和控制设备控制器—设备接口（CDI）第 3 部分：DeviceNet》。我国的 ODVA 组织（ODVACHINA）是中国电器工业协会通用低压电器分会现场总线（DeviceNet）工作委员会的简称，由上海电器科学研究所牵头成立，目前正

积极推广该技术。

DeviceNet 设备层的网络。可将基本工业设备（如限位开关、光电传感器、阀组、电动机起动器、过程传感器、条形码读取器、变频驱动器、物料流量计、电子秤、显示器和操作员接口等）与 PLC 连网，从而避免了昂贵和繁琐的硬接线。在减少了配线和安装工业自动化设备的成本和时间的同时，还提供有设备级诊断功能。据统计报告，已有超过 40% 的最终用户在他们的网络中选择使用了 DeviceNet。

除了 DeviceNet，OBVA 组织还开发了用于控制层的 ControlNet 网络。它在同一物理层介质链路上提供时间关键性 I/O 数据和报文数据，以及程序的上传/下载，组态数据和端到端的报文传递等通信支持。它使用隐式令牌网技术，具有确定性、可重复性、可靠性、同步性、协调性和实时性。ControlNet 已为成为 AB PLC 控制网络的主体。其基本原则也被 OMRON PLC 控制网（ControlNet Link）所采用。

随着以太网技术的进步，ODVA 还开发有主要用于信息层，同时也可用于控制层与设备层的 EtherNet/IP 标准。它定义了一个开放的工业标准，将传统的以太网与工业协议相结合。该标准是由国际控制网络（ControlNet International，CI）和开放式设备网络供货商协会（ODVA）在工业以太网协会（Industrial Ethernet Association，IEA）的协助下联合开发的，并于 2000 年 3 月推出。EtherNet/IP 是基于 TCP/IP 系列协议，因此采用以原有的形式 OSI 层模型中较低的 4 层。所有标准的以太网通信模块，如 PC 接口卡、电缆、连接器、集线器和开关都能与 EtherNet/IP 一起使用。

2005 年，ODVA 为适应“位”一级数据可靠通信的需求，还推出 CompoNet 网络，以满足在众多传感器与执行器之间的应用需求。不过 AB 公司目前还没有这样的产品。倒是 OMRON 公司捷足先登，于 2006 年就推出这个网络。

以上 4 种网络组成 CIP（Common Industrial Protocol，原称为控制和信息协议）网络家族。其顶层都使用通用工业协议 CIP。这个协议包含了面向各种制造自动化应用的信息和服务组合，其中包括控制、安全、同步、运动控制、配置以及信息。作为与传输媒介无关的独立协议，被世界上数以百计的开发商所支持，CIP 给制造业用户带来了统一的通信架构。它的 EtherNet/IP 还可用于网络实时控制，可集成到设备级，能给用户提供诸多优势。同时，这个网络家族可通用配置，可跨越几个网络及收集和控制数据，并连到全球互联网或公司内部网，在所有工作级上提供连续的信息流。EtherNet/IP 为用户提供网络工具，使他们能够在因特网以及企业内网上以标准的以太网技术来设置其制造应用要求，所得到的结果是：无论何时何地都可获取数据信息。

2. Profibus 标准

Profibus 由德国 13 家工业企业及 5 家研究所于 1984 年开始研制，20 世纪 90 年代初成为德国国家工业现场总线协议标准，代号 DIN19245。1996 年经欧洲电工委员会批准被列为欧洲标准 EN50170。根据欧洲标准化规则，EN50170 于当年自动地在法律上得到欧洲所有国家标准化机构的认可。德国注销了原有的 Profibus 国家标准 DIN19245，以 EN50170 取而代之。从现在起，欧洲所有公开的招标都是在 EN50170 的基础上进行的。EN50170 在保护投资方面为生产厂家和用户提供了一个最高的标准。

Profibus 提供一个从传感器一直到管理层的透明网络。正因为如此，Profibus 可以在许多方面——从汽车工业、机器制造业、食品工业、运输业直到环保工程等获得应用。作为开放

式通信系统工业标准，Profibus 现场总线公布了网络各层协议的所有规范。按照这些规范设计设备网络接口，不同的设备可以实现网络互连。这给控制设备的生产厂家、系统设计安装调试单位和用户带来了极大的方便。

目前 PNO（Profibus 用户组织）已拥有 600 多个成员，生产近千种产品。Profibus 的核心公司为：Siemens 公司，E + H 公司，Samson 公司，Softing 公司等。根据 1997 年统计，世界上已有 100 多万台 Profibus 仪表在自动化设备中应用，而且每年增长 20% ~30% 。目前，世界上约有 650 家厂商加入了 Profibus 用户协会并提供上千种 Profibus 产品。以著名的西门子公司为例，它可提供 100 多种 Profibus 产品，并已经把它们应用在中国的许多自动控制系统中。

为在中国推广应用 Profibus 标准，Profibus 中国用户协会于 1997 年 7 月成立。协会的会员由生产厂商（包括国际 Profibus 用户协会成员在中国开办的合资或独资企业）、科研单位、学校、厂矿企业及其他用户组成。协会的宗旨是竭诚为广大用户服务，通过举办技术讲座及发行不定期内部刊物等手段介绍国际国内 Profibus 发展及应用的最新动态，宣传和介绍有关生产厂家的最新产品及应用实例，促进用户之间的信息交流。2001 年 11 月 2 日 Profibus 协议被正式批准为中华人民共和国机械行业标准 JB/T 10308. 3—2001。

此外，Profibus 国际组织（Profibus International，PI）后来又推出 Profinet。是新一代基于工业以太网技术的自动化总线标准。作为一项战略性的技术创新，Profinet 为自动化通信领域提供了一个完整的网络解决方案，可覆盖诸如实时以太网、运动控制、分布式自动化、故障安全以及网络安全等当前自动化领域，并且作为跨供应商的技术，可以完全兼容工业以太网和现有的现场总线（如 Profibus）技术，以保护现有投资。

在底层的设备网络，还有流行于欧洲的 AS-i（操作器传感器接口）标准，使用得也很广泛。

3. CC-Link 标准

CC-Link（Control & Communication Link）全称为控制与通信总线，是 1996 年 11 月以三菱电机为主导的多家公司以“多厂家设备环境、高性能、省配线”理念开发、公布和开放了的现场总线标准。它不但具备高实时性、分散控制、与现场设备通信、RAS 等功能，而且依靠与诸多现场设备制造厂商的紧密联系，提供开放式的环境。

2002 年，CC-Link/LT 问世。它可与 CC-Link 无缝连接。擅长于位通信，可接小规模的（1 ~16 点）通信模块。提供更简单的接线、更小的 I/O 尺寸、更低的接线成本，面向小点数的分散系统，适用于传感器-执行器层的网络。

2003 年，CC-LinkVer. 2. 0 推出。在原来 CC-Link 的基础上，将数据通信容量最大扩大了 8 倍，满足了仪表和控制中的“多路模拟-数字数据通信”等需要大容量和稳定的数据通信领域的要求，增加了它的吸引力。

随着以太网技术进步及其在 PLC 中的应用，CC-Link 协会还最新提出了基于以太网的整合网络“CC-LinkIE”，不但可以控制，而且可以进行设备管理（设定、监视），设备维护（监视和故障检测），数据收集（动作状态）等。不仅能满足当今飞速发展的制造业对高速且大容量的工业用网络的需求，而且也能很好地实现从信息层到现场网络的纵向整合，提供了从信息层到现场设备级网络的无缝通信。

为了开展 CC-Link 现场总线在全球的普及和推进工作，2000 年 10 月，Woodhead、Cont-

ec、Digital、NEC、松下电工、三菱等6家常务理事公司发起，在日本成立了独立的非盈利性机构“CC-Link 协会”（CC-Link Partner Association，CLPA）。截止2004年1月，CLPA会员累计达550家公司，其中海外会员达278家，已累计推出551种CC-Link兼容产品。至2003年，全球已累计销售217万个CC-Link站点。

于2001年4月，CLPA在中国设立CC-Link推广中心（CC-Link Promotion Center，CLPC），负责中国（包括香港地区）的CC-Link技术全面推广和对CC-Link成员的支持工作。2008年12月27日，中国自动化学会集成自动化技术专业委员会控制与通信网络CC-Link工作组（CLPA China）在上海成立。CLPA China将作为在中国发展与推广CC-Link技术的主要机构，负责CC-Link中国会员的发展、常规会员兼容产品的开发、一致性测试的实施以及CC-Link在中国的普及推广，同时将依托专委会的平台，促进CC-Link与中国国内高等学府、设计院、企业和自动化各界展开更广泛深入的合作。

4. Modbus 标准

Modbus由美国Modicon公司（后被法国施耐德电气公司收购，现为后者的一个品牌）在1978年发明，是全球第一个真正用于工业现场的总线协议。截至2004年，Modbus的站点安装数量已经超过了800万个，且75%的产品为非施耐德电气产品。安装的地区遍及世界各地。Modbus的巨大成功，可以归结到以下4个方面：

（1）标准开放

用户可以免费、放心地使用，不用交纳许可证费，也不会侵犯知识产权。

（2）面向消息的协议

可以支持多种电气接口，如RS-232、RS-422、RS-485等，还可以在多种介质上传送，如双绞线、光缆、无线射频等。要说明的是：和很多的现场总线不同，它不用专用的芯片与硬件，完全采用市售的标准部件。这可保证采用Modbus的产品造价最为低廉。

（3）协议的帧格式是最简单、紧凑、高效、通俗易懂

用户使用容易，厂商开发简单。用户和厂商可以通过www. Modbus-IDA. org网站和其他网站，下载各种语言的样例程序、控件，以及各种Modbus工具软件，更好地使用Modbus。

（4）具有安全可靠的通信能力

1989年Modicon公司在Modbus基础上又开发推出了新一代的Modbus+网络，以满足用户和市场的需求。Modbus+也以Modbus为基础，它采用了令牌传递、对等方式、即插即用的网络结构，为用户提供了更快的工业网络。

1998年施耐德公司又推出了新一代基于TCP/IP以太网的ModbusTCP，目的是满足用户和市场的进一步要求。ModbusTCP是第一家采用TCP/IP以太网用于工业自动化领域的标准协议，是至今唯一获得IANA赋予TCP端口的自动化通信协议。因特网上前1000个端口都已分配给著名的、公开的通信协议，如80号口分配给了著名的HTTP（超文本传输协议），供因特网浏览器使用。这说明，ModbusTCP是标准的、开放的、免费的通信协议，这也秉承了施耐德公司的一贯做法，为用户提供了新的选择。

ModbusTCP的应用层还是采用Modbus协议，简单高效；传输层使用TCP协议，并使用TCP502号口，用户使用方便，连接可靠；网络层采用IP协议，因为因特网就使用这个协议寻址，故ModbusTCP不但可以在局域网使用，还可以在广域网和因特网上使用。

要强调的一点的是，ModbusTCP 全部采用标准的以太网硬件！因为目前一些厂商对标准以太网进行了改进，所以不能使用市售的产品，势必增加了用户成本，而施耐德向用户承诺：决不使用特殊硬件，确保用户选择的自由度。

目前的 ModbusTCP 以太网的速度为 10M/100Mbit/s，大大提高了数据传输能力。除此之外，施耐德的以太网解决方案 TCP/IP 以太网还为用户提供了更多的服务，如 I/O 扫描、全局数据、故障设备替换、网络管理、电子邮件报警、时钟同步等功能，为用户带来更多的附加值。

为了更好地普及和推动 Modbus 在基于以太网上的分布式应用，目前施耐德公司已将 Modbus 协议的所有权移交给 IDA（Interface for Distributed Automation，分布式自动化接口）组织（总部设在美国），并成立了 Modbus-IDA 组织，为 Modbus 今后的发展奠定了基础。

Modbus-IDA 组织是一个非盈利、独立的、基于 web 的社团。其任务是鼓励自动化设备的独立使用者和制造商，采用 Modbus 通信协议，使用分布式自动化架构，为多个市场提供相应的产品。Modbus-IDA 将提供基础平台，使用户能得到和共享协议、应用和认证信息，最终降低使用的成本。

在我国国内也有很多的用户，如和利时 PLC，就支持和使用 Modbus 的标准。2008 年，《基于 Modbus 协议的工业自动化网络规范》正式成为国家标准，编号为 GB/T 19582—2008。Modbus 成为国家标准后，用户将极大地受惠于使用国家规范的服务；自动化生产厂家所生产的设备将在全球范围畅通无阻。

1.5　PLC 网络及其配置

关键词：DeviceNet、CopomNet、ControlNet、EtherNet/IP、Profibus、Profinet、AS-i、CC-Link、CC-Link/LK、CC-Link IE、PLC 网络配置

研究网络基础知识及各种模型、协议，目的是更好地了解 PLC 网络，并做好 PLC 网络配置。这个配置也是 PLC 系统配置的重要组成部分。一般也都是在进行 PLC 系统配置时一并考虑。其任务是根据应用要求，确定 PLC I/O 点数、类型、型号及与 PLC 通信的对象，通信要求，进而再选定 PLC 网络类型、接口模块、通信介质及必要网络组件，以求得在处理好 PLC 其他配置的同时，也求得 PLC 网络的最优解决方案。

PLC 网络配置的目的是实现数据通信。对象不同，通信的目的不同，选择网络的类型及对网络性能的要求也不同。这些都将影响在网络配置时对解决方案的选定。此外，由于网络兼容性的原因，一般讲，同一网络只能使用同一品牌的网络产品。所以，它的配置还与 PLC 品牌、型号紧密相关。

为了讨论，以下先简要介绍几个品牌 PLC 的网络概况，以及 PLC 网络的一般特点，然后再介绍 PLC 网络配置。

1.5.1　PLC 网络概况

以下将对各主要厂家的现行 PLC 网络作简要介绍。

1. OMRON PLC 网络概况

日本 OMRON 公司 PLC 产品很多。当前主流产品为 CPM2A、CPH1、CP1E、CP1L、

CQM1H、CJ1H 及 CJ2H（小型机的尺寸，但具备中型机的控制规模）、CS1H（虽为中型机，但控制点数可达 5000 多点）、CS1D（可双机热备）及 ZEN（微型机，有可编程继电器之称）。

图 1-44 所示为 OMRON 公司 PLC 网络示意图。分有 3 级。企业级为信息层（主要是以太网），用于 PLC 与计算机连网。车间级为控制层（主要是 ControllerLink 网），用于 PLC 与 PLC 连网通信。现场级为设备层（主要是 DeviceNet、CompoNet 网），用于主、从 PLC 之间或 PLC 与现场设备连网通信。这 3 级网络可互连，办法是，用若干具有不同网络接口的站点，分别接入不同网络得以实现。

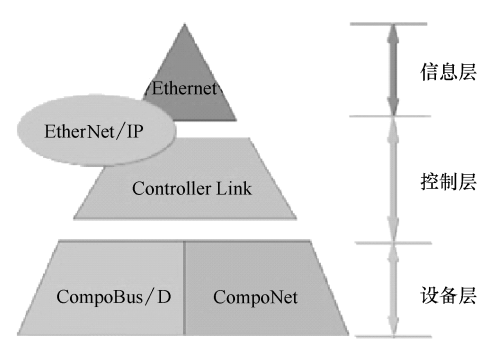


图 1-44　OMRON 公司 PLC 网络示意图

图 1-45 所示为 OMRON 公司 PLC 网络详图。它把设备层与控制层结合在一起，都称为网络控制。其特性见表 1-12。

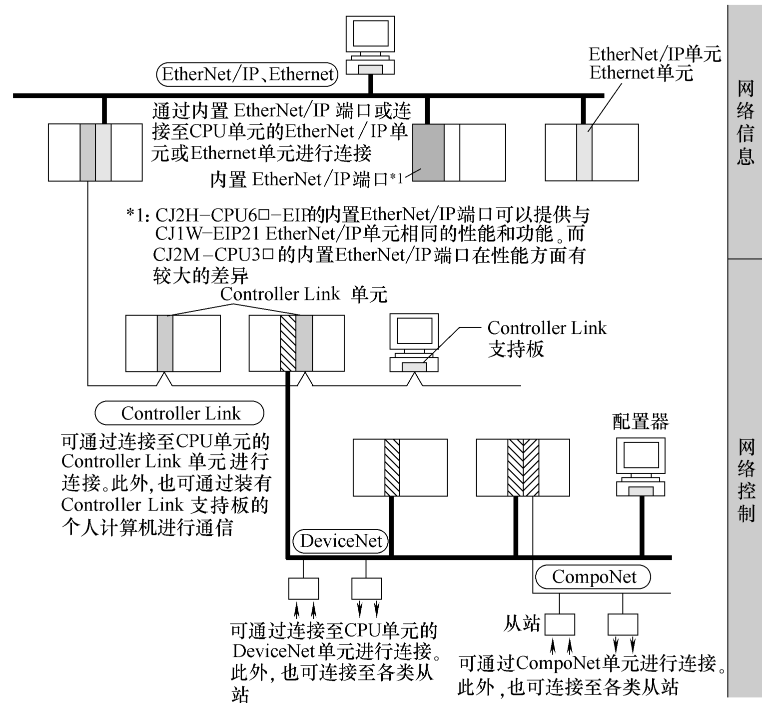


图 1-45　OMRON 公司 PLC 网络详图

（1）以太网

有多种版本，如 10Base-5、10Base-T、100Base-TX 等。10Base-5 用的传输介质为同轴电缆，速率 10M，总线结构。10Base-T、100Base-TX 为非屏蔽双绞线，速率分别 10M、100M，星形结构。后者的功能也比前者强，但可与前者兼容。

100Base-TX 版本新。不仅连网方便、成本低、与旧版本兼容；而且，通信速度为原来的 10 倍。还新增了 E-MAIL 及 Socket 等原来所没有的功能。所以，是 OMRON 目前主推的

以太网方案。最新推出的还有 CS1W-EIP21 和 CJ1W-EIP21 以太网模块，与 Ethernet/IP 标准接近，也可支持数据链接通信（说明见后）。通信速度及能力比过去的高出多倍。支持的通信协议也有增多。

表 1-12　OMRON PLC 网络特性

系统	网路	功能	通信	通信设备
信息网络	EtherNet/IP	上位计算机和 PLC 之间	FINS 报文通信	CJ2H-CPU6 □-EIP 或 EtherNet/IP 单元的内置 EtherNet/IP 端口
		PLC 之间		
		上位计算机和安装在 CPU 单元中的存储卡之间	FTP 服务器	
	Controller Link	PLC 和直接连接到通信网络的个人计算机之间	FINS 报文通信	Controller Link 支持板或 Controller Link 单元
			数据链接(偏移量,简单设定)	
	RS-232C→Controller Link	上位计算机和通信网络中的 PLC 之间	上位链接指令和网关	RS-232C 电缆和 Controller Link 单元
控制网络	EtherNet/IP	PLC 之间	标签数据链接	CJ2H-CPU6 □-EIP 和 CJ2M-CPU3□上的内置 EtherNet/IP 端口或 EtherNet/IP 单元
	Controller Link	PLC 之间	FINS 报文通信	ControllerLink 单元
			数据链接(偏移量,简单设定)	
	DeviceNet		开放式网络中的 FINS 报文通信	Device Net 主站单元和配置器
	DeviceNet	PLC 和网络设备(从站)之间	开放式网络中的大容量远程 I/O(固定或自由分配)	DeviceNet 主站单元和配置器
	CompoNet		开放式网络中的高速、多点、多节点远程 I/O	CompoNet 主站单元

OMRON 以太网可以是简单的局域网，也可为互联网，还可冗余配置。同一 PLC 可配置两个以太网，一个工作，一个备份。一旦前者出现故障，后者将自动地无缝接替。冗余配置以太网的传输介质也是双绞线，速率也是 100M。其功能除了冗余，其他与非冗余的基本相同。冗余以太网使用的模块也可配置成没有冗余的，故可与没有冗余的兼容。

当然，不是 OMRON 的所有 PLC 都可接入以太网。只是可配置有以太网模块或集成有以太网接口的高档机型才可接入。

（2）Controller Link 网

是 OMRON 公司于 20 世纪 90 年代后期开发的 PLC 控制网，用于 OMRON 中、大型机及高档小型机，如 CP1H。如果计算机配置有 Controller Link 网卡，也可与计算机连网。

Controller Link 网是工业级的。可靠性高，但建网的成本也高。所以，仅与计算机连网通信时，一般不使用它。

Controller Link 网所用的模块型号很多。通信介质可以是双绞线，也可为光纤，还可建冗余网络，较常用的是 CLK21 版本。它用双绞线作为传输介质，可用重复器增大距离。还可通过光电转换器转换为使用光纤作为传输介质，以增大传输距离。

Controller Link 网站点数一般为 32 个，也可扩展为 64 个。通信速率可选定。与距离及传输介质有关，如使用屏蔽双绞线为传输介质，500m 时为 2Mbit/s，1km 时为 500bit/s。而且它的通信方法多。交换的数据量大，一次通信可提交几 k 的数据。

（3）DeviceNet 网

是主从网，在 PLC 间连网主要是用在大、中型 PLC（设为主站）与小型 PLC（设为从站）间通信。也可配置远程分布系统，用于 PLC 与现场设备及传感器/执行器通信，以实现 PLC 对现场设备及智能装置的信息采集与工作控制。

OMRON PLC 这类网络有 ComboBus/D 网（符合 DeviceNet 网标准），ComboBus/S 网，（OMRON 自身标准）。推荐使用 DeviceNet 网。

（4） CompoNet 网

这是继 DeviceNet 之后按 ODVA 新公布的标准开发的网络。也是主从网。通信的站点更多，速度也更快，距离也更长。但通信的帧较小，可按位通信，更适合底层 I/O 设备连网。

除了上述网络，利用标准串口也可实现 PLC 与计算机、PLC 与 PLC、PLC 与现场设备连网通信。性能虽差些，但较经济、简便，也很常用。对 C 系列机，串口的通信用 HostLink 协议，是公开的。对 CS 系列机还可用 FINS 协议，也是公开的。

近期，OMRON 还生产有可接入其他网络（如 Profibus 网络）的网络接口模块。这可使它的 PLC 与其他网络互联、互通。

2. AB PLC 网络概况

美国 AB（Allen-Bradley）公司创建于 1903 年，在世界各地有 20 多个附属机构，10 多个生产基地。近年，AB 公司推出 Logix 系列 PLC 产品，把 PLC 技术推向新的高度。这些型号为

ControlLogix 最多可控制 12800 个 I/O 点，或 4000 路模拟量。

FlexLogix 最多可控制 256 个 I/O 点。输入输出模块可以放置在传感器和执行器附近，分布在不同的链路上。如果有分布式处理需求，可以对多个 FlexLogix 控制器进行连网。

CompactLogix 最多可控制 128 个 I/O 点。

MicroLogix 为小型机，仅能控制几十点。

PicoLogix 为微型机，控制点数更少，为小巧型控制器。

此外，还有软 PLC（SoftLogix5800Controller），过程控制 PLC（Programable Process Controller，PPC）及安全性（GuildPLC） PLC。

AB 公司的 ControlLogix 性能最高，它集中了 Logix 通用平台的多种优点——通用的编程环境、通用的通信网络、通用的控制引擎——提供了一个既能满足您高性能应用需求又易于使用的环境。它具有以下优点：每个 ControlLogix 控制器可以执行多个控制任务；可以在一个机架上使用多个处理器、通信模块和输入输出模块，ControlLogix 处理器、输入输出模块、通信模块就像网络上的智能站点。等等。

AB PLC 网络使用 NetLinx 开放式网络架构，也分为三级：以太网 EtherNet/IP、控制网 ControlNet、设备网 DeviceNet。此外还有远程输入输出 UniversalRemoteI/O，如图 1-46 所示，可实现从车间级到顶级无缝连网。

Ethernet/IP（以太网）使用标准的以太网、TCP/IP 技术和一种名叫 CIP（Control and Information Protocol）的开放性应用层协议。CIP 也是 DeviceNet 和 ControlNet 网络的应用层协议。这个开放性的应用层协议使得面向自动化和控制应用的在 EtherNet/IP 上的工业自动化和控制设备的互操作性和互换性成为现实。

ControlNet 是一种开放性的、工业的、实时控制级网络。可提供控制器与输入、输出设备及驱动、操作员界面、计算机或其他设备间的连接，并且能整合 DH + 网络（AB 专有控

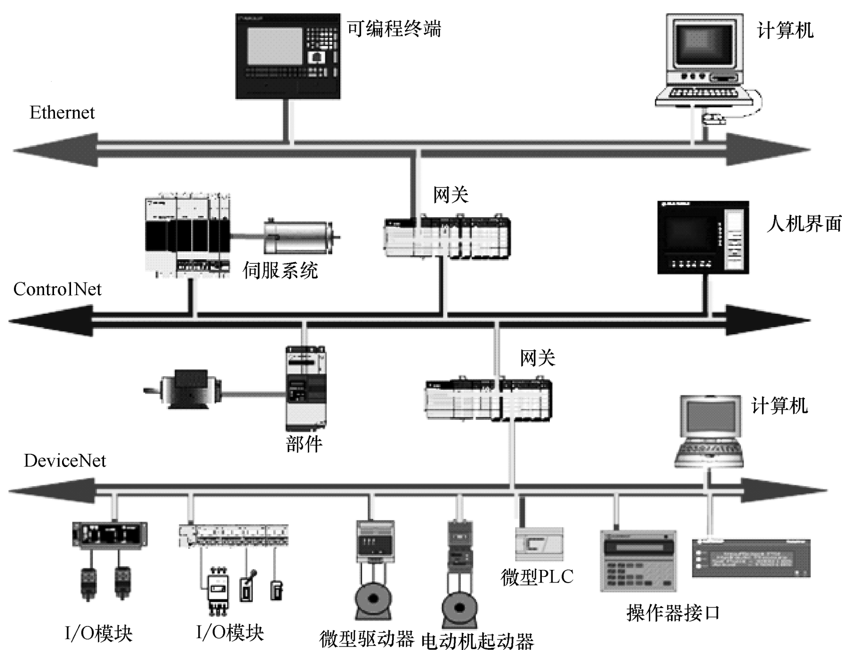


图 1-46　AB 公司 PLC 网络

制级使用）和远程输入输出等现存通信方式。

DeviceNet 是一种低成本连接工业设备（如限位开关、光幕、多向阀、电动机起动器、过程传感器、条码阅读器、变频器、显示界面和人机界面等），可以用主/从、多主/从、点到点或者三者的组合来组建。用它可减少昂贵硬件布线费用，可提供设备的诊断信息。它使用生产者/消费者网络模式。具有实时控制数据交换与配置能力。

AB 网络的重要特点是采用了 NetLinx 开放式网络架构，是开放的连网技术。在这个架构下，利用它提供的网络管理软件——RsLink，不必设定路由表，就可自动寻找路径，实现三层网络 DeviceNet、ControlNet 和 EtherNet/IP 无缝连接。同时，还可采用统一的网络协议，共享一组相同的通信服务。该协议也就是通用工业协议（Common Industrial Protocol，CIP），能够使用户在任何 NetLinx 网络上方便实现控制、系统组态和采集数据。

NetLinx 可给用户带来很多利益，如便于数据和信息的传送，减少编程，减少带宽压力，提高了系统响应的时效，无需额外的电缆，提高了生产率，等等。

3. 西门子 PLC 网络概况

德国西门子公司的 PLC 产品很多。当前主流产品为 S7 系列机，有 S7-200、1200（小型），S7-300、1300（中型）及 S7-400 机（大型）。性能比 S5 大有提高。此外，还推出微型机 Logo。控制点数很少，但其继电器的输出容量很大，输出电流可达 8A，可直接带动执行器，也有可编程继电器之称。

西门子 PLC 最简单的网络是用 CPU 模块上集成的标准通信串口建立 PPI、MPI 网。它不仅可用于计算机与 PLC 连网通信，也可实现 PLC 与 PLC、PLC 与现场设备连网通信。PPI 使用的协议为西门子的 PPI 协议。可通过运行程序设定，把某 S7-200 站点设为主站。此时，设为主站的 S7-200 机，可以用网络读（NETR）和网络写（NETW）指令，读、写其他 CPU

中的数据。此外，还可通过运行程序设定串口为自由端口模式。这时，其通信协议由用户定义。并可使用中断、发送指令（XMT）和接收指令（RCV）等与通信对象交换数据。MPI 网可使用全局数据设定的方法，实现 S7-300、400PLC 之间的通信。

而最有效的方法还是使用有关通信模块或集成接口，组成相应通信网络。西门子 PLC 可组成的网络也是 3 级，如图 1-47 所示。工业以太网为信息网，Profibus 网主要为控制网，也可用于设备层连网，而设备级则有 AS-i 网及 KNX 网。

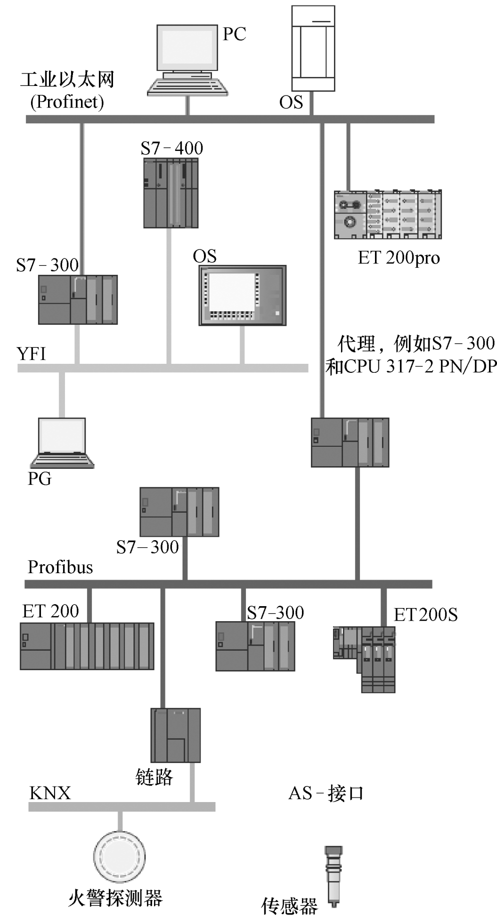


图 1-47　西门子 PLC 网络

Profinet——它的早期为 10M 以太网，后来为有交换功能，全双工和自适应的 100M 波特率快速以太网（FastEthernet，符合 IEEE802. 3u 的标准）。近期发展为工业自动化领域内开放的工业以太网标准，采用 TCP/IP 技术，支持实现分布式自动化结构。可通过以太网集成简单的分布式现场设备以及运行等时运动控制应用。

Profibus——是国际标现场总线标准之一，并占有重要地位。可以满足两类通信应用（制造应用和面向过程的应用）。还允许在运行过程中对现场设备进行参数化和优化，从而缩短机器重组时间。其设备诊断功能也有助于缩短工厂停机时间。

AS-Interface——是执行器-传感器-接口的英文缩写，是有国际标准可依的最底层的设备级的总线主从网络。主要用以实现 PLC 向开关量的传感器和执行器读写数据。这些传感器可以是位置接近、温度、压力、流量、液位开关等；执行器可以是各种开关阀门、声、光报警器、继电器、接触器等低压开关电器等。模拟量的传感器和执行器也可与其连接，但通信要多周期完成，实时性不佳。

KNX 是 Konnex 的缩写，是在 1999 年 5 月提出的总线协议，提供了家庭、楼宇自动化的完整解决方案，也是楼宇自动化的全球标准之一。接到 KNX 介质上（这些介质包括双绞线、射频、电力线或 IP/Ethernet）的总线设备，可以进行数据交换。这些总线设备主要是用于控制楼宇管理装置，如照明、遮光/百叶窗、保安系统、能源管理、供暖、通风、空调系统、信号和监控系统、服务界面及楼宇控制系统、远程控制、计量、视频/音频控制、大型家电等。所有这些功能通过一个统一的系统就可以进行控制、监视和发送信号，不需要额外的控制中心。但它在工业控制中用得不多。

西门子 PLC 连网能力很强，即使小型机也如此。如 S7-200 机就集成或可配置几乎所有的西门子网络接口或模块，具体如图 1-48 所示。

利用这些接口或模块，除了可实现进行计算机与 S7-200CPU 之间连网，做编程通信，

还可实现多种连网与通信。例如：S7-200CPU 之间连网与通信；S7-200 与 S7-300/400 之间的连网与通信；S7-200 与西门子变频器间的连网与通信；S7-200 与其他上位机软件间的连网与通信；S7-200 与第三方 PLC 之间的连网与通信；S7-200 与第三方 HMI 之间的连网与通信；S7-200 与第三方变频器之间的连网与通信及 S7-200 与其他串行通信设备之间的连网与通信，等等。

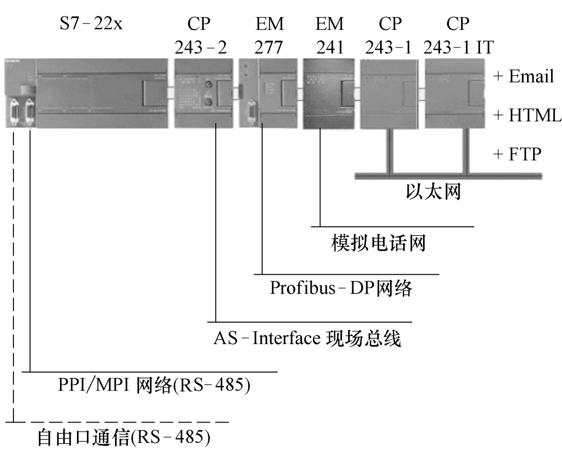


图 1-48　S7-200 集成或可配置网络接口或模块

4. 三菱 PLC 网络概况

日本三菱公司 PLC 产品很多。当前主流产品为 FX 系列机、Q 系列机及 Alpha 微型机。最近还推出功能介乎 Q 与 FX 之间，性能更强的 L 型机。此外，在三菱公司 Q 系列高档机中，除了有常规的顺序控制 CPU 外，还推出运动控制 CPU、过程控制 CPU 及 PC（计算机）CPU，分别可进行运动控制、过程控制及信息处理。

三菱把工厂网络分为办公自动化网络（OA）与工厂自动化网络（FA）。前者用通信回路将公司内部的计算机连接在一起，以求得办公室业务的高效化的信息类（OA）网络，后者用通信回路将工厂内部的生产设备、装置等连接在一起，以求得生产的自动化、高效化的控制类（FA）网络。它的网络级的结构如图 1-49 所示。

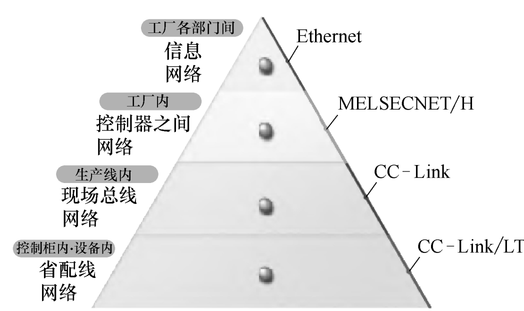


图 1-49　三菱网络级结构

图 1-50 所示为它的网络详图。这里实际也是把 PLC 网络归结为信息系统及制造系统。前者为以太网，后者为控制及设备网，用了各种 CC-Link 系统。中间靠 CC-Link IE 搭桥。所有网络站点都可用无缝信息协议交换数据。

（1）以太网

处于企业网络的顶级，信息（OA）网络。可将公司事务部门（人事、财务、营业、资材等）、技术部门（设计等）的计算机、服务器，以及打印机等 OA 设备用通信回路连接在一起，并通过服务器实现信息的管理与共享，以及各种 OA 设备的共用，可提高各个部门的业务效率。此外，而且还能连接各种 FA（工厂自动化）设备，在 PLC、设备控制器以及生产管理用 PC 之间传输生产管理信息、质量管理信息及设备的运转情况数据。它的 Q 系列 PLC 系列的 Ethernet 模块具有了日益普及的因特网电子邮件收发功能，使用户无论在世界的任何地方都可以方便地收发生产信息邮件，构筑远程监视管理系统。同时，利用因特网的 FTP 服务器功能及 MELSEC 专用协议可以很容易地实现程序的上传/下载和信息的传输。

（2）控制网

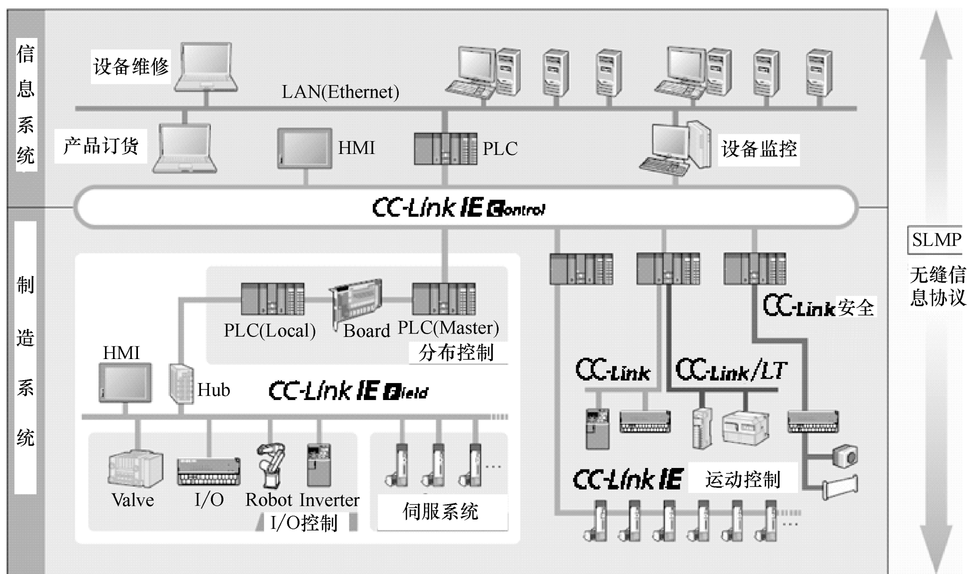


图 1-50　三菱 PLC 网络详图

传统的为三菱的 MELSECNET/10（H）网，是整个网络系统的中间层，在 PLC、CNC 等控制设备之间方便且高速地进行处理数据互传的控制网络。作为 MELSEC 控制网络的 MELSECNET/10，以它良好的实时性、简单的网络设定、无程序的网络数据共享概念，以及冗余回路等特点获得了很高的市场评价，被采用的设备台数在日本达到最高，在世界上也是屈指可数的。而 MELSECNET/H 不仅继承了 MELSECNET/10 优秀的特点，还使网络的实时性更好，数据容量更大，进一步适应市场的需要。但目前 MELSECNET/H 只有 Q 系列 PLC 才可使用。此外，CC-Link、CC-Link IE 也可作为它的控制网。而且由于它的性能好，又合乎事实标准，已出现用得越来越多的趋势。

（3）设备网

除了 CC-Link，还有 CC-Link/LT，用以把 PLC 等控制设备和传感器以及驱动设备连接起来的现场网络，为企业网络基础。采用 CC-Link 及 CC-Link/LT 可大大减少布线数量，提高了系统可维护性。而且不只是 ON/OFF 等开关量的数据，还可连接 ID 系统、条形码阅读器、变频器、人机界面等智能化设备，从完成各种数据的通信，到终端生产信息的管理均可实现，加上对机器动作状态的集中管理，使维修保养的工作效率也大有提高。

另外，除了拥有上面所提到的网络之外，有的还可支持 Profibus、Modbus、DeviceNet、AS-i 等其他厂商的网络，还可进行 RS-232/RS-422/RS-485 等串行通信，通过数据专线、电话线进行数据传送等多种通信方式。

5. 施耐德网络概况

施耐德 PLC 有多个品牌，如 Modicon TSX、Twido 等。在 Modicon TSX 品牌中，有 Quantum（昆腾）、Premium、Momentum、Compact 及 Micro 等。最高档主流机型为昆腾。图 1-51 所示为它的相关的网络。

从图知，它的网络也是 3 级结构。最高一级为管理层，用的是工业以太网，负责 PLC 与计算机传输生产管理信息。中间层为控制层，目前也用以太网，可使用 Modcon TCP/IP 协议（也支持 AB 开发的 Ethernet/IP 协议）通信，也可实现 PLC 的冗余配置（CPU 热备）。最

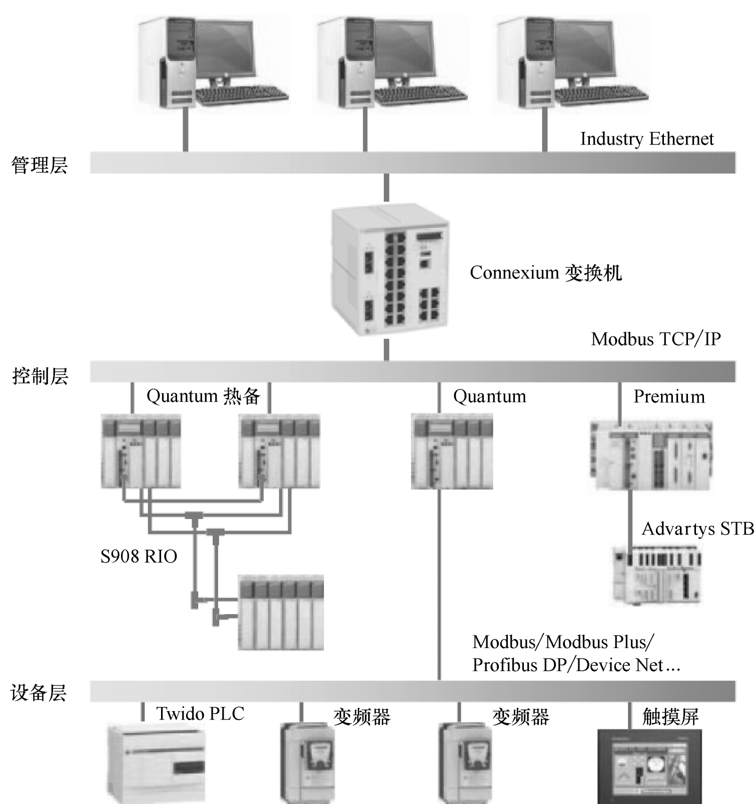


图 1-51　施耐德 PLC 网络

下一级为设备层，为现场总线，使用远程 I/O 链路，采用周期 I/O 方式通信，负责 PLC 与现场设备的通信。设备网支持的协议有它自身的 Modbus +（Plus）或者 Modbus 网，也支持 Profibus、DeviceNet、AS-i 及 Interbus-s 等多种通信协议。

Modbus 协议是原美国 MODCON 公司开发的，现已成为开放的网络通信协议。其 Modbus RTU 通过标准串口很容易实现，在工控行业得到了广泛的应用，已不仅是一个 PLC 的通信协议，在智能仪表，变频器等许多现场设备都有相当广泛的应用。

6. GE PLC 网络概况

美国的通用电气公司（GE）与日本的数控之王 FANUC 公司合并成立了 GE-FANUC 公司。其当今 PLC 主流产品有 PAC 70、90-70、90-30 及 VersaMax。PAC 性能最高，也称可编程自动化控制器。而 VersaMax 是近期开发的 VersaMax 是 GE Intelligent Platforms 公司推出的新一代控制系统。是具有“三合一”功能的系列产品：既可作为单独的 PLC 控制机，具有可接受的价格和优越的性能；又可作为 I/O 从站，通过现场总线受控于其他主控设备，如 GE90-70、90-30 以及第三方 PLC、DCS 或计算机系统；还可构成由多台 PLC 组成的分布式大型控制系统。

GE PLC 支持工业以太网。使用自身的 SRTP TCP/IP、EGD 及开放的 Modbus TCP/IP 协议。其自身的以太网协议内容不对外公开，但它提供有 SDK 开发包，可以基于该开发包通信程序。可以用以太网在 PLC 与计算机之间、PLC 与 PLC 之间、PLC 与远程 I/O 及人机界面之间通信、交换数据。图 1-52a 所示为它的以太网概况。

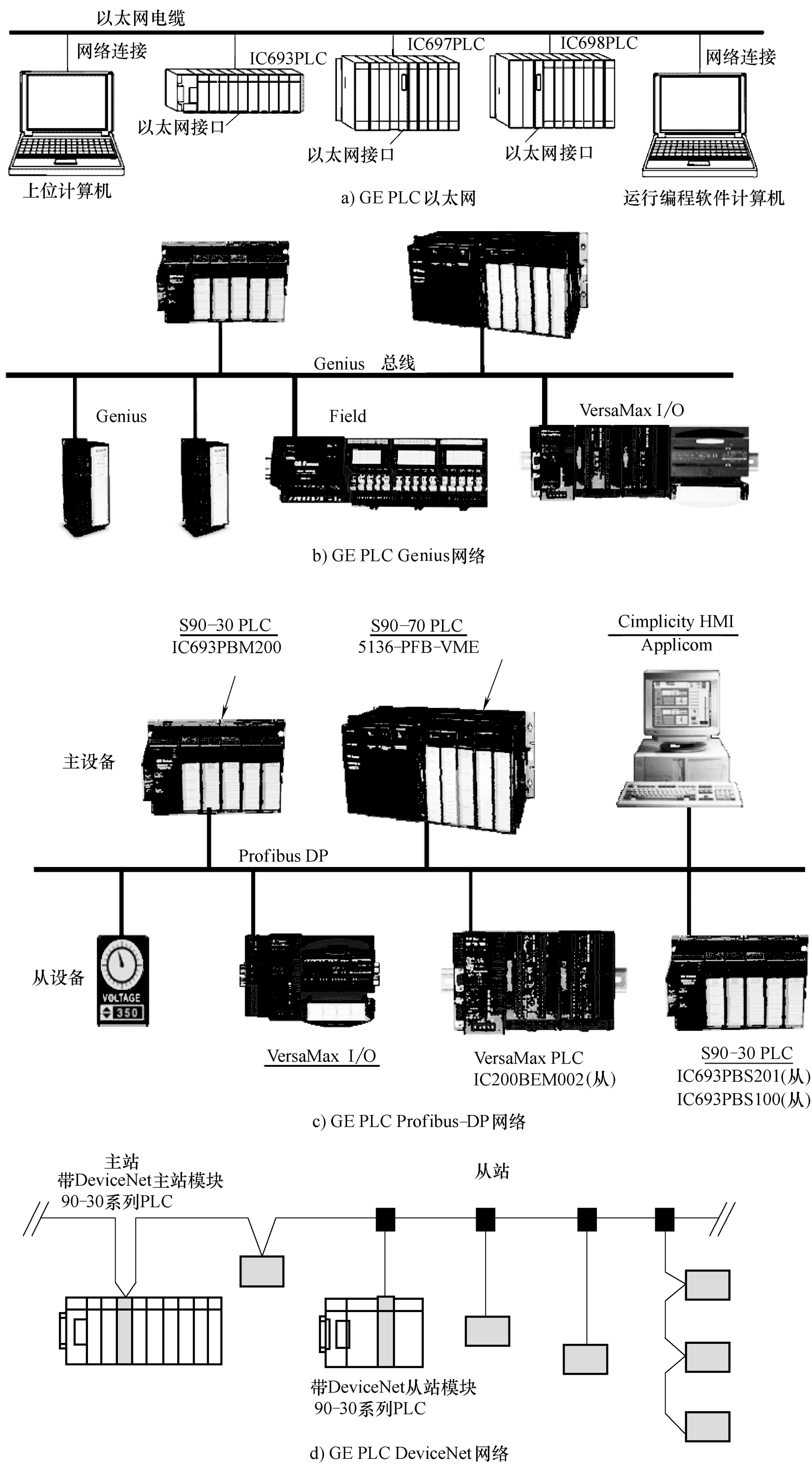


图 1-52　GE-FANUC 公司的 PLC 网络

GE FANUC 于 1985 年还开发了 Genius 网。可用于分布 I/O 的控制，与 PLC 的远程 I/O 相当。同时，还支持 PLC 之间通信。所使用的为自身专有的令牌通信协议。一个网络最多可有 32 个站点。通信介质可采用屏蔽双绞线、光纤或 Modem。网络传输能力为：当距离为 2300m 时，速率可达 38.4KB/s；距离为 605m 时，为 153KB/s。同时还支持冗余配置，支持 PLC 全系统的冗余。图 1-53b 所示即为 Genius 网络概况。

GE FANAC PLC 还支持多种开放的 PLC 网络，如 Device Net、Profibus-DP 等。图 1-53c、d 所示即为这两种网络接入概况。

7. ABB PLC 网络概况

ABB 由成立于 1883 年的瑞典阿西亚公司（ASEA）和成立于 1891 年的瑞士布朗勃法瑞公司（BBC Brown Boveri），在 1988 年合并而成。集团总部位于瑞士苏黎世。是电力和自动化技术领域的领导厂商。ABB PLC 开发业较早，当今主流机型是 AC（Advance Control）500 及 AC31。前者为模块式的大、中型机，后者为箱体式小型机。具体型号很多。软件完全符合 PLC 行业标准，很便于客户使用。它的有多种通信接口或模块，入网选择的范围广。除了自身的 CS31 分布式 I/O 网络外，其他的 PLC 现场总线标准网络，它多可接入。图 1-53 所示为它的网络概况。

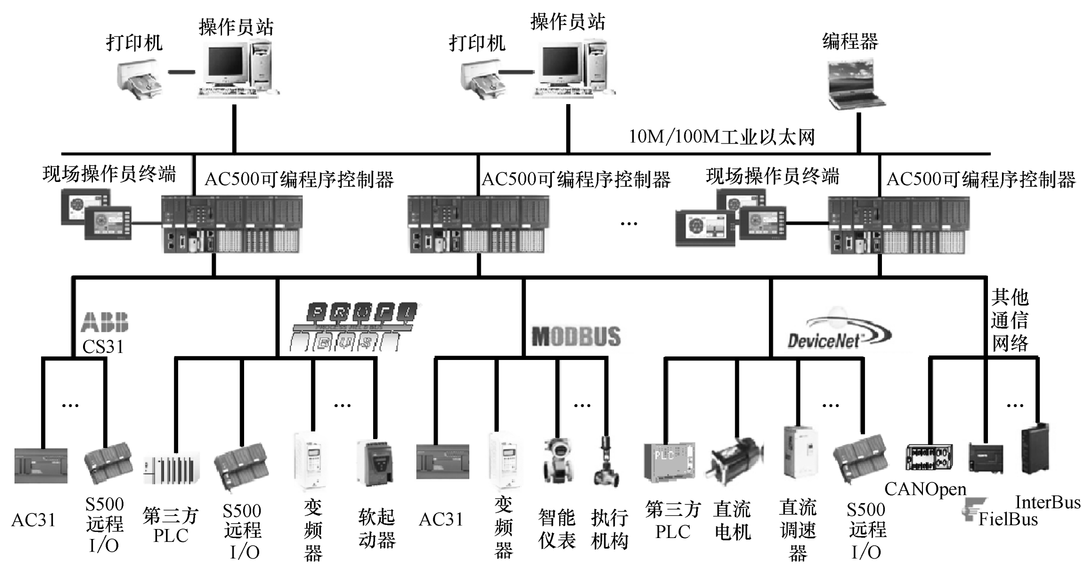


图 1-53 ABB PLC 网络

从图知，它与计算机通信用的是工业以太网，支持 ProfiNet、EtherCat 等协议。同时，这工业以太网还可用于 PLC 间通信。而现场总线除了 CS31，可以为 Profibus、MODBUS、DeviceNet 以及其他现场总线网络。

8. 和利时 PLC 网络概况

和利时公司 PLC 是国产（大陆产）产品。开发虽晚，但起点高、功能较强、性能也较好。它的特点是：程序语言标准化；内部器件变量化；指令系统组合化；模块设定软件化；程序组织模块化；编程监控一体化。它没有自身单独协议的 PLC 网络。但是，它的 PLC，如 LM 机，其 CPU 模块集成有标准 Modbus 协议和自由协议串行通信接口。此外，还有其他

与当今流行协议兼容的通信模块，如 Profibus-DP、Ethernet（使用 Modbus TCP 协议）、DeviceNet、LonWorks、CANopen、FF、Modem、GPRS/GSM 等。运用这些兼容模块，可十分方便地接入这些网络。

图 1-54 所示为它的 LM 机接入局域网的概况。

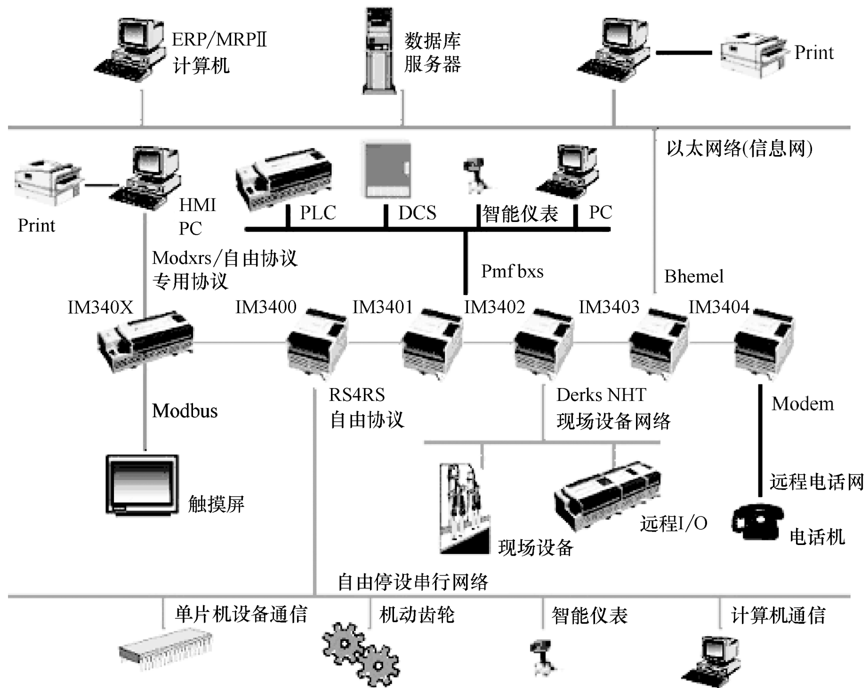


图 1-54 和利时公司 PLC 网络接入概况

从图知，从与现场设备连网、到与其他控制器连网，从接入当今最流行的以太网，到通过电话网络通信，LM 机都可实现、都可配置。这样，LM 机虽然没有自身独立的网络协议，但也可以避免使自身成为“信息孤岛”。

1.5.2 PLC 网络特点

从以上介绍可知，PLC 网络大体有如下一些特点：

1. 类型多、差别大

PLC 网络与普通计算机网络相比，其网络的类型要多得多。原因来自它的站点类型多。除了计算机站点比较单一，而 PLC 站点、现场设备站点的品牌、类别、型号则是多种多样的。也因此给它的网络赋予不同的功能与结构。

PLC 网络类型很多还由于它的网络多是 PLC 厂家专用的。几乎一个厂家一个样。即使开放的网络，由于标准多，又各推广各的，造成了即使是开放网络类型也很多的情况。

PLC 网络不仅类型多，而且网络的差别还很大。不同标准、品牌网络有差别，同一标准、品牌新旧版本的网络也有差别。

网络类型多虽然给网络配置提供更多的选择机会，但差别大给网络的使用、维护增加了难度，而且给网络互连、互通也带来很大不便。

要指出的是，同一公司 PLC 不同网络之间，只要有一个或多个 PLC 安装有可连接这不同网络的相应模块，并用它做网桥，一般都可实现这些网络站点间的互连、互通，交换数据、相互操作。只是有的要设定路由表，有的要有专用软件。

2. 要求高、造价贵

PLC 网络与普通的计算机网络相比，对其要求要高得多。

首先，PLC 网络多用于实时控制，特别它的控制网络及设备网络更是如此。因此对其通信的延时不能太长，通信的确定性也要有保证。否则将影响系统控制的实时性与精确性。

其次，PLC 网络多在现场使用。工作环境恶劣，受各种干扰影响，易出故障。为此，要求网络能适应恶劣环境，抗干扰能力要强。

再就是，如果出现故障，为了减少损失，要求系统能很快修复。为此，要求网络要便于诊断，便于维修。

最后，为了安全及数据保密，更不允许在其上传播“病毒”或“黑客”入侵，以确保系统的数据及控制进程的绝对安全。

正是对 PLC 网络要求高，为了满足这么高的要求，各个 PLC 厂家都做了大量投入对其进行研究，因而所开发的网络产品价格自然比普通计算机网络产品要高得多。特别它的专用网络由于批量小，更是如此。价格高对 PLC 网络的推广与普及自然也是一个不小的限制。但是，有的 PLC 信息网，如果处于企业的现场高层，也可考虑选用普通计算机网络的组件。这既可降低造价，又便于维修。事实上，很多 PLC 厂家也是这么推荐的。

3. 发展快、前景光明

PLC 网络与普通的计算机网络相比，其发展速度更快些。因为它既受计算机网络技术进步的影响，还受 PLC 自身产品升级换代的推进。它的落后的网络正在逐步淘汰，新的性能正不断推出。各个厂家当前主流网络与当初的传统网络都已大不相同。

其次是，随着计算机与 PLC 工作速度的提升，PLC 网络速度也不断加快。如后推出的设备网 CompoNet 与早推出的设备网 DeviceNet，尽管前者的“档次”要低些，但其网速还比后者高了不少。这也是 PLC 网络的一个重要趋势。不论信息网、控制网或设备网，后推出的网络速度几乎都比原有的要高些。

可贵的是，虽然 PLC 网络类型多、差别大，难以互连、互通，但随着网络标准化的推进及各大公司间的协调与妥协，已出现网络趋同的趋势。网络标准的类型在减少，目前基本上已集中于推广几个用户占有率较高的若干网络。而且不少大公司不仅生产自身主推的标准网络产品，也生产其他公司主推的网络产品。使自身的 PLC 也可接入其他标准的 PLC 网络。如三菱公司，它的主推网络产品是 CC-Link，但它也生产 Profibus、AS-i 等其他网络产品，为自身 PLC 与这些网络互连、互通创造了条件。

再就是，一些公司虽没有自身的网络体系与标准，但可使用若干个市场占有率高的开放网络标准，开发自身网络，使自身的 PLC 也可接入这些网络，如国产和利时 PLC，就是这样，它开发有 Profibus 等模块，其 PLC 就可接入 Profibus 等网络。这样的结果就使自身的 PLC 就不会成为当今信息化时代的“孤岛”了。

还有就是，由于开放标准的发展，不断出现有这样公司，它专门生产实现 PLC 网络的互联、互通网桥模块。这样模块，一边用于连接一家，如 AB PLC 网络，另一边用于连接另一家，如西门子 PLC 网络。有了这样连接不同网络的模块也就可实现两个不同 PLC 网络站

点间的互连、互通，交换数据、相互操作。

最后还要指出的是，由于工业以太网通信速度的不断提高及技术的完善，通信的可靠性大为增强，以太网通信的实时性已不再令人担心。所以，近来几乎各个级（层）的设备大多也配备有以太网接口。所以，以上介绍的 3 级（层）网络，都使用以太网是完全可能的。这样，PLC 网络配置既可降低成本，又可提高兼容性，变得简单与方便了。也许这将是将来 PLC，甚至其他工业网络发展的一个趋势与新的亮点。

1.5.3　PLC 网络配置

PLC 网络配置是一个复杂的系统工程。要与 PLC 现场的控制系统、工厂的信息系统一并考虑。涉及 PLC 选型、网络选型、现场设备选型、站点分布、通信介质确定、通信实现等一系列软硬件问题。

1. PLC 网络配置任务

1）根据配置站点的现场设备、I/O 点数及工艺要求，做好这些站点 PLC 的自身配置。

2）根据现场控制及 PLC 控制协调的要求，确定要配置的网络类型并做好各个类型网络的配置。同时还要确定这些网络的互连。各个类型网络配置的具体内容包括网络规模（站点数）、覆盖范围、拓扑结构、网络组件、通信介质以及通信协议、通信软件。

3）根据配置要求采购、安装、接线，并做好站点硬件设定。

4）用网络工具软件做好网络设定（组态）及在线测试。

5）编制应用与通信程序。

2. PLC 网络配置原则

为了配置好 PLC 网络，以取得更大的效益，一般要遵循如下几个原则：

1）针对性原则。要合理确定所配置网络的功能，并按功能需要做好配置。要做到有的放矢，既不要达不到功能要求，也不要功能多余。

2）实时性原则。要合理确定网络的实时性、确定性。通信的确定性是一定要保证的。而实时性，对设备网、控制网，是首先要满足的要求；对信息网，由于在大多数监控系统中，对数据的采集和处理速度要求也较高。

3）可靠性原则。要确保所配置的网络工作可靠。要根据工作环境确定防护等级，按防护要求选定网络部件。

4）全面性原则。PLC 网络配置只是 PLC 配置一部分，PLC 网络也只是企业网络的一部分，所以，它的配置既要与 PLC 一起考虑，也要与企业的网络配置协调。这样，将确保能以较少的投资，取得企业自动化、信息化综合效益。

5）先进性原则。当今 PLC 网络技术发展很快，应当尽量选用技术水平高、有发展前途、短期内不会被淘汰的网络。还要特别注重考虑网络的开放性，要优先选用开放网络。这将更便于与企业其他网络的互连互通。

6）经济性原则。经济是一切活动的基础。进行 PLC 网络配置当然要考虑经济，考虑到投资的合理性，如系统的性价比、投入产出比、企业的经济承受能力等因素。

3. PLC 网络配置类型

PLC 网络是分类的，对其配置当然也要分类进行。

（1）设备网配置

用于 PLC 与现场设备通信。主要考虑现场设备的数量（I/O 点数）、分布（地点、距离）工作环境等情况。如果这些设备比较集中，设备与 PLC 距离又不大，可以不用这类网络。但如果 PLC 可控制 I/O 点数不足，需要用远程 I/O 网络来增加可控制规模的则另当别论了。如果这些设备比较分散，有的设备与 PLC 距离又较大，可以考虑使用这类网络。

设备网有两种，一是更底层的网络，如 AS-i、CC-Link 或 CompoNet 网，适用于站点很分散，各个站点多是开关量，点数又不多的系统；另一是层次稍高点的网络，如 DeviceNet 网、Profibus 网、CC-Link 网等，适用于站点也很分散，但各个站点既有开关量，又有模拟量的系统。目前还可考虑也选用工业以太网。

（2）控制网配置

用于 PLC 与 PLC 通信。有两种情况，一是协调 PLC 间的控制，二是扩大 PLC 控制规模。前者交换的数据量有限，只要通信的确定性有保证，时延又不是太长的控制网络都可以选用。后者交换的数据量要略大些，在确保通信确定性的同时，最好选用网速较高的控制网络。

控制网一般与 PLC 的品牌是对应的。PLC 配置时，选用什么品牌的 PLC，控制网多是什么品牌的控制网络。目前也还可考虑选用工业以太网。

（3）信息网配置

用于 PLC 与计算机通信。其网络配置有几种情况：

1）仅仅用于编程。一般使用串口网络或 USB 口就可以了。

2）要实现 SCADA 功能，可使用串口网络。如果要提高网速可使用信以太网。

（4）网络互连配置

网络互连有两层意思：一是同类网络互连；另一是不同类网络互连。前者主要看企业自动化要求。如果企业自动化规模很大，要多个生产线协调工作，而仅仅一个网络又难满足要求。这时可能进行网络互连，如两个或多个控制网互连。后者主要看企业信息化的要求。如果企业信息化推进很快，管理层从现场采集信息与向现场发送指令的工作很多，那么凡是涉及与管理数据的现场设备的设备网、控制网都要与信息网互连。

网络互连的方法主要是通过可以连接两个或多个网络的 PLC 实现。这样的 PLC 实际是身兼两职，既要用于控制，又要作为网桥，实现两个或多个网络的互连、互通。

4. PLC 配置步骤

1）根据 I/O 点数及工艺要求做好 PLC 自身配置。

2）根据现场设备分布情况确定是否配置设备网。如果需要，则针对需求选定网络类型并做好配置。

3）根据协调控制或扩大控制规模的需要确定是否配置控制网。如果需要，则针对需求选定网络类型并做好配置。

4）根据信息采集与处理的需要确定是否配置信息网。如果需要针对需求选定网络类型并做好配置。

5）根据现企业网络的发展需要确定是否进行网络互连。如果针对需要选定相关网桥站点，并做好相关配置。

5. PLC 网络配置实例

（1）PLC 网络基本配置

主要用于 PLC 编程，是 PLC 必不可少的网络配置。没有这种网络，PLC 无法编程，也无从工作。最常用的是使用串口网络。这种配置几乎为零成本。因为这里除了电缆，网络接口都是现成的。只是编程软件要由 PLC 厂家提供。目前，也有用 USB 口取代原标准串口，也很方便，同时速度更快。这种网络只是需要编程时联网，程序下载及调试完成后可以不连网。所以，这种网络实际是“临时”网络，不总是在线的。

如果要实现 SCADA 功能，也可使用这个网络。应用程序或使用组态软件，或由用户编写。而为了实时实施监控，网络也必须总是在线。

由于 PLC 以太网成本的降低，为了提高速度，实现编程及 SCADA 功能也有使用以太网的。也许将成为未来的趋势。

（2）PLC 网络应用配置

目前 PLC 应用广泛，可用作顺序控制、过程控制、运动控制、信息控制及远程控制。PLC 网络应用配置就是围绕着 PLC 这些应用的需要所做的配置。应用配置只是按需要做的，不是非配置不可。

用于顺序控制、过程控制、运动控制、远程控制的网络配置主要看 PLC 现场设备的分布及控制协调的需要，主要是设备网及控制网选用。这样实例很多，本书将随着这些网络的介绍，逐步予以介绍。

用于信息控制主要是信息网（目前主要是以太网）的选用及设备网、控制网与它互连。最终目的是能把现场的信息上传到企业的信息层，企业信息层的指令能下达到现场，使企业实现信息化，已取得更大的效益。这样的实例也很多，本书将随着这些网络的介绍，逐步予以介绍。

1.6　PLC 网络通信实现

关键词：地址映射通信、地址链接通信、生产者、消费者通信、协议通信、自由协议通信、套接字服务通信、OPC 通信、web 通信

有了 PLC 网络，不等于网络上各个站点间的就能自行交换数据。这里还要有相应的设定（有的称为网络配置或组态），有的还要运行通信程序，才能实现数据通信。而通信的实现机制则与具体的网络有关。同一网络可能有多种机制。同一种机制也多可用于不同的网络。本节将介绍各种 PLC 网络站点之间常用的通信机制。

1.6.1　自动通信

这种机制是经过网络组态，不必运行通信程序，或只运行串口设定程序，各站点即可通信。多用运于 PLC 站点之间通信，非常可靠，也非常方便，具体有 3 种形式。

1. 地址映射通信

用于 PLC 主从网络中站点之间通信。

图 1-55 所示为一个主从网络的实例。图中 1 为主 PLC 上的远程主控单元或接口，为通信主站。而 2、6 为从 PLC。3、7 分别为从 PLC 2、6 上的 PLC I/O 链接或从站单元，为通信从站。图中的 4、5 为主 PLC 的远程 I/O 终端，无自身 CPU，分别作为主 PLC 的 I/O 点受主 PLC 管理。

远程 I/O 终端与主 PLC 虽有通信，但它不是独立站点。作为主 PLC 的 I/O 点，在逻辑上与主 PLC 当地的 I/O 点没有区别。所差的只是 I/O 的响应时间略有通信所需的若干毫秒的延迟。

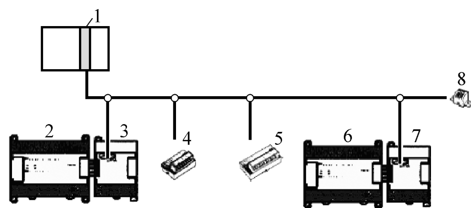


图 1-55　主从网络
1—主 PLC 上的远程主控单元　2、6—从 PLC　3、7—PLC I/O 链接单元　4、5—主 PLC 远程 I/O 终端　8—网络终端器

从站 PLC 有自身的 CPU，还有自身的 I/O，对其自身 I/O 的控制完全由自身管理。要与主站 PLC 交换信息，必须通过交换数据实现。这里的关键是使用了 PLC I/O 链接或从站单元。它既是从 PLC 的扩展模块，在从 PLC 中有其 I/O 地址；又是主 PLC 的远程 I/O 终端，在主 PLC 中也有其映射的 I/O 地址，如图 1-56 所示。

以图示为例，从站 1 的读（输入）区（字）10，在主站上的映射地址为 1000。从站 2 的读（输入）区（字）10（不一定非是 10），在主站上的映射地址为 1002，且都是主站的写（输出）区（字）。从站 1 的写（输出）区（字）11，在主站上的映射地址为 1001。从站 2 的写（输出）区（字）11（不一定非是 11），在主站上的映射地址为 1003，且都是主站的读（输入）区（字）。可知，每个从站在主站中都有专用于通信的数据读写映射地址。

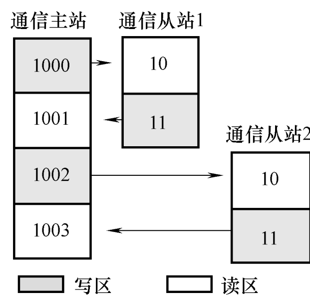


图 1-56　地址映射通信机理示意

这样，当主站轮流与各个从站及远程 I/O 终端通信时，将把主站映射区的数据依次发送给对应的从站输入区，各从站输出区的数据也依次返回给主站对应的映射区。而从站之间、主站远程 I/O 终端之间、从站与主站远程 I/O 终端不能通信，不能交换数据。

在这样系统中，如果从站 1 的 PLC 要向主站 PLC 发送数据，其具体过程可分为 5 步：

1）把要向主 PLC 传送的数据，写入通信用输出区（如从站 1 为的内存字 11）；

2）通过从 PLC 输出刷新，把数据传到 PLC I/O 链接单元或从站单元的存储区（如从站 1，为字 11 的地址）；

3）通过网络通信，把 PLC I/O 链接单元或从站单元存储区的数据，送主站主控单元的存储区（字 1001 的映射区）；

4）通过主 PLC 输入刷新，主站主控单元存储区的数据，被读入主 PLC 的地址映射区（主 PLC 的字 1001）；

5）主 PLC 从地址映射区（主 PLC 的字 1001）读取这个数据。

主 PLC 向从 PLC 发送数据的过程与此过程相反。先是主 PLC 向映射区写数据；再经主 PLC 输出刷新，传入主站主控单元的存储区；再通过网络通信，传入从 PLC I/O 链接或从站单元存储区；再经从 PLC 输入刷新，传到从 PLC 的输入存储区；最后由从 PLC 读取这个数据。

这里说的很复杂。但这里的输出、输入刷新都是 PLC 操作系统自动实现的。这里的 PLC I/O 链接单元与主 PLC 主控单元间的数据传送，是由远程网络通信系统自动完成的。而且其通信过程如同 PLC 的扫描过程一样，总是周而复始地重复着。

这种通信，用户所要做的只是编写有关的数据读写程序。只是它所交换的数据量不大。多只有一对输入、输出通道，故只能用于较底层的网络上。

图中的 4、5 是主 PLC 的远程 I/O 终端，不是从 PLC，是直接受主 PLC 控制。所以，这种网络也是 PLC 远程 I/O 系统的延伸。OMRON 称之为远程 I/O 链接，是主、从 PLC 网络。被链接的从 PLC，有自身的 CPU，可独立运行程序，可进行实际控制。只是为了与主 PLC 交换数据，才与主 PLC 连网。

此外，OMRON 的 DeviceNet（即 COMMBO/D）及 COMMBO/S 网，三菱的 CC-Link 网，西门子的 Profibus 网也有这样类似地址映射机制，也可用此方法通信。

采用地址映射通信，输出对输入的响应是有延时的。从以上对它的通信过程叙述就可看出，具体的不再赘述。

提示：用数据区地址映射通信只能在主站与从站之间进行。而从站之间通信则要通过主站转达。

提示：主站 PLC 及各从站 PLC“写区”、“读区”的大小取决于使用什么样的网络平台及作什么样的设置（组态）。

提示：PLC 远程 I/O 系统系统，从站没有 CPU，不能自行控制。控制的成本虽低，而一旦通信出现故障，从站的控制将无法实现。

2. 地址链接通信

又称数据链接（Data Link）通信，也是用数据单元通信，只是这参与通信的数据单元在通信各方用相同的地址。三菱称之为循环通信（Cyclic Communication），多用于控制网。西门子的 MPI 网把它称为“全局数据包通信”。发送数据的站点用广播方式发送数据，同时被其他所有站点接收。而那个站点成为发送站点，由“令牌”管理。谁拥有“令牌”，谁就成为发送站点。这个“令牌”实质是二进制代码，轮流在通信的各站点间传送。无论是管理网络的主站，还是被管理的从站，都同样有机会拥有这个“令牌”。其通信机理如图 1-57 所示。

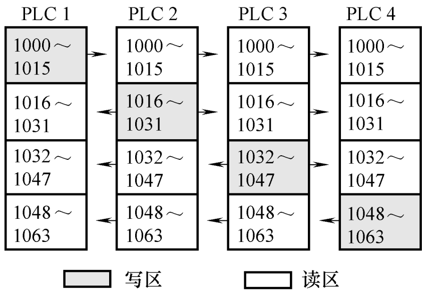


图 1-57　链接通信机理示意

该图为 4 个 PLC 进行数据链接通信的示意。字地址 1000 ~ 1063 之间的 64 个字被设置作为这个链接的数据区。而每个 PLC 都把它的这个区分为写与读两个部分。且这个划分对每个参与链接的 PLC 都是互补的。如 PLC1，其“写区”为 1000 ~ 1015 字，“读区”为 1016 ~ 1063 字，则 PLC2 的“写区”为 1016 ~ 1031 字，“读区”为 1000 ~ 1015 字及 1032 ~ 1063 字，等等。

这 4 个 PLC 的数据链接通信分 5 步实现：

1）运行程序，把要向外传送的数据写入自身的写数据区；

2）输出刷新，把“写区”数据传到 PLC 链接单元或接口的对应（写）缓冲区；

3）参与 PLC 链接的 PLC 链接单元或接口间相互传送数据，把各链接单元或接口对应（写）缓冲区的数据传给其他 PLC 的 PLC 链接单元或接口的对应（读）缓冲区；

4）输入刷新，把 PLC 链接单元或接口缓冲（读）区的数据读入到读数据区；

5）运行程序，把要使用的数据从自身的读数据区读走。

这里的输出、输入刷新是在程序扫描开始前或结束后由系统自动实现。必要时，也可在程序中加入 I/O 刷新指令实现，以加快程序对链接数据的响应速度。

这里的各 PLC 链接单元或接口间的数据传送，则由 PLC 链接系统的网络通信自动完成的。其通信过程如同 PLC 的扫描过程一样，总是周而复始地重复着，力求使各 PLC 链接单元的存储区的数据保持一致。

说得通俗一点，这里设置的链接数据区相当于邮局的信箱。数据发送与接收如同发信与收信。要外送的数据先投（写）入信箱，靠信箱的传送机制，把数据传送给对方。要用的数据则从来自别的 PLC 数据的信箱中取出。其间的数据传送如同邮局为你服务一样，会自动实现的。若要快速传送，可另作 I/O 刷新，这如同寄快信一样。

总之，这个通信数据交换，经历了两种过程：

一是 PLC 的内存区中“链接区”与 PLC 链接单元或接口的缓冲区之间数据交换。这是由 I/O 刷新实现的。其周期取决于各 PLC 的程序扫描周期或程序中使用 I/O 刷新指令的情况。

二是各 PLC 链接单元或接口间的数据交换。它由主站 PLC 管理“令牌”，进而使各 PLC 轮流把链接单元或接口缓冲区中“写区”的数据，传送给其他 PLC 的“读区”。

这两个过程各按照各的周期重复进行着。也正是有了这两个过程，PLC 间的数据交换才成为可能，而且非常可靠。

链接通信交换的数据量比较大，可以为几个、几十字，是很常用、很方便的 PLC 间的对等通信的方法。具体大小取决于链接数据区的大小及参与链接的 PLC 数量。

提示：参与链接的不一定都是 PLC，只要配置有相应的通信硬件，如计算机上安装有 OMRON ControlLink 网络通信板及相关驱动程序，也可与连网的 PLC 链接通信。

3. 生产者、消费者通信

生产者/消费者间通信用于 AB PLC 网络。也是在网络组态时，先对生产者/消费者的标签作设定。这标签即变量，可与硬件地址相关，也可无关。标签可设为生产者，也可设为消费者。然后把设定下载给相关 PLC。当这些 PLC 都处运行状态时，生产者标签即可根据设定的时间间隔或现值变化的情况，向同名的所有消费者标签传递它的现值，之间的通信即可自动实现。设定为生产者的 PLC 的相关标签提供数据。设定为消费者的 PLC 的相关标签消费，即读取数据。可知，它的基本机理于数据链接类似。只是它的设定更加灵活。其好处还在当建立多站点连接时，一个报文同时可被多个接收站点同时接收，既可保证数据使用的同步，又不必向不同站点多次发送相同的报文，大大节省网络的带宽。

1.6.2　对话通信

站点间通信靠相互对话实现。要发起者通信的站点，先运行通信程序，发送通信命令，通信对方接收命令后，或由它的操作系统应答及处理，或运行人工程序应答及处理。针对不同通信网络有以下 3 种形式。

1. 自由协议通信

多用在串口连网的平台上。通信双方根据自行约定，调用串口通信指令进行通信。也称无协议通信。

自由协议通信用于 PLC 之间通信，双方都要有串口通信指令。用于 PLC 与计算机，双

方都要编程。主要是串口读、串口写。有的还要串口设定及使能。后两者用于串口初始化。当然，这个设定与使能有的也可用编程软件完成。

要弄清的是，执行读、写指令只是对 PLC 串口缓冲区的读、写。而数据发送及接收则是 PLC 通信管理系统分时完成的。一般讲，PLC 用于处理通信的时间大体占其程序扫描时间的 10% ~20%。所以执行数据发送指令后不是马上就把数据发送出去的。反之，不执行接收指令也不等于 PLC 不接收数据。只是把收到的数据放入接收缓冲区。

提示：只要串口的物理电气、功能特性相同，双方又同处于可使用自由协议通信，那么，使用各自的串口指令，还可以在不同品牌 PLC 间进行通信。

2. 串口协议通信

也是用于串口连网通信。主动方根据被动方的通信协议，向被动方发送通信命令；被动方接收到命令后，不必运行通信程序，而由操作系统处理通信命令，并按要求向主动方应答。

显然，这里弄清通信协议是关键。否则主动方无法编程。在串口连网平台上，计算机与 PLC 通信、PLC 与现场设备通信多是用协议通信。

3. 网络协议通信

在 PLC 网络或有的串口连网的平台上，主动方（PLC 或计算机）按网络协议，执行网络通信指令，与被动方 PLC 通信。它交换数据量大，可达几百个字节；通信速度快（取决于网络底层特性）。而且只要有网关，有的还可跨网络通信，即网络中继运作（Network Relay Operations）。

网络通信指令有读、写及操作命令。主动方发送命令，被动方不需执行任何指令，都可对指定网络、指定站址、指定数据区进行读或写。可向对方发送操作命令，使对方改变工作模式。可强制或复位对方是工作位及文件操作等。

但是，被动方也可执行保护自身的指令。执行后，可不让对方读、写自身数据，或受其操作。

网络协议通信要建立在 PLC 网络的平台上，而这样的平台各厂家 PLC 多互不兼容。因此用这样的通信只能在同类型 PLC 间进行。

4. 套接字（Socket）服务通信

用于 PLC 以太网络通信，要用到套接字技术。套接字原是计算机应用程序使用 TCP 和 UDP 协议的接口技术。而 OMRON PLC 的以太网也支持这个技术，以实现 PLC 与计算机以及 PLC 与 PLC 间通信。而且在使用这个技术时，要预先做好 PLC 的设定，然后设法把套接字激活或调用网络通信命令进行通信。

PLC 的套接字通信服务支持 UDP（无连接通信），也支持 TCP（有连接通信）。也还可执行 FTP（文件控制传输）协议，以在计算机与 PLC 进行文件传输。

1.6.3　专用软件通信

专用软件用于计算机与 PLC 间连网通信。并多可在多种通信平台使用。专用软件通信的好处是不必弄清 PLC 的通信协议，不用编程或较容易也较简单编程即可通信，有的还可用于 PLC 编程及网络设置。但要计算机上装载这些软件、函数、控件或运行通信服务程序。

1. PLC 厂家提供编程软件通信

PLC 厂家编程软件除了可以用于脱机编程，还可用于与 PLC 联机。可对 PLC，甚至 PLC

网络进行设定（或称配置、组态），下载、上传 PLC 程序，读写 PLC 数据以及改变 PLC 工作状态。有的 PLC 编程软件还有监控数据动画图形显示功能。所有 PLC 厂家都提供有这类软件。只是多数要收费，但有的是随着购买 PLC 免费赠送。

使用这些软件时要注意有关版本的消息。如西门子 S7-200 用编程软件经历了一个长期的发展过程，从 STEP7-Micro/DOS（DOS 下运行）到 STEP7-Micro/WIN16（运行于 16 位 Windows 下），一直到现在的 STEP7-Micro/WIN32（可在 32 位 Windows 操作系统下运行）。但 Micro/WIN32 只是说明它适用于 32 位 Windows，而不是版本号。现在 Micro/WIN32 就简称 Micro/WIN。常见的 Micro/WIN 版本有 V4.0 和 V3.2。在每个版本中，还会有小的升级，以 SPx（ServicePack）表示。不同版本的 Micro/WIN 生成的项目文件不同。高版本的 Micro/WIN 能够向下兼容低版本软件生成的项目文件；低版本的软件不能打开高版本保存的项目文件。其他厂家编程软件情况也类似。建议尽可能使用最新版本的软件。

2. PLC 厂家提供网络管理软件通信

PLC 厂家除了提供编程软件，一般还提供专用于网络配置、测试与管理的软件。例如 OMRON CX-one 软件包中的 Integrator 就是网络配置工具。可用以网络配置、通信及测试。CX-one 中的其他工具软件多也可用以与 PLC 通信。

有的 PLC 厂家还提供专用于通信的软件，也可与 PLC 通信。有了它，用户程序再与其做动态数据交换，即可间接与 PLC 通信。

3. PLC 厂家提供有通信接口函数通信

API 函数原是微软在设计 Windows 操作系统时加进去的。PLC 厂家提供的 API 则是 PLC 厂家适应 Windows 操作系统开发的，专用该厂家 PLC 与计算机通信的函数。与厂家专用通信软件不同的是，这些通信函数不能单独运行，是要嵌入到用户的程序中，由应用程序调用才可工作，才能实现计算机与 PLC 的通信。

使用 API 的好处是不必弄清 PLC 的通信协议，但要在计算机上装载相关的驱动。

4. PLC 厂家提供有通信控件通信

控件是很多 PLC 厂家都开发有可为可视化编程软件使用的，针对自身 PLC 串口或网络模块的通信控件（ActiveX 控件）。如 OMRON、三菱 PLC 都有专门通信控件。用户的应用程序可调用这些控件，即可实现与 PLC 通信。

使用控件的好处也是不必弄清 PLC 的通信协议，但要在计算机上装载这些控件。

5. OPC 通信

在 16 位 Windows 时代，程序间通信用的是动态数据交换（Dynamic Data Exchange，DDE）。两个 Windows 应用程序同时运行。其中一个作为服务器（Server），另外一个作为客户（Client）。后者向前者发送服务请求，后者将予以回应，从而实现两个程序之间的数据交换。现在已进入 32 位 Windows 时代，DDE 当然用得很少了。

现在程序间通信用的是 OPC（OLE for Process Control）。它诞生于 1996 年 8 月。随着 1997 年 2 月 Microsoft 公司推出 Windows95 支持的 DCOM 技术，1997 年 9 月新成立的 OPC Foundation 对 OPC 规范进行修改，增加了数据访问等一些标准，使 OPC 规范得到了进一步的完善。

OPC 是 OLE 在工业控制领域的应用。而 OLE（Object Linking and Embedding）指对象链接与嵌入技术，是应用程序间传输和共享信息的一组综合标准。所以，OPC 是微软处理程序间通信、数据交换的新技术，是 DDE 在 32 位 Windows 时代的新发展。

OPC 基础委员会主席 Dave Rehbein 是这样描述 OPC 的，即 OPC 基于 Microsoft 公司的 Distributed Internet Application（DNA）构架和 Component Object Model（COM）技术的，根据易于扩展性而设计的。OPC 定义了一个工业标准接口，这个标准使得 COM 技术适用于过程控制和制造自动化等应用领域。

具体地讲，OPC 是以 OLE/COM 机制作为应用程序的通信标准。OLE/COM 是一种客户/服务器模式，具有语言无关性、代码重用性、易于集成性等优点。OPC 规范了接口函数，不管现场设备以何种形式存在，客户都以统一的方式去访问，从而保证软件对客户的透明性，使得用户完全从低层的开发中脱离出来，为基于 Windows 的应用程序和现场过程控制应用建立了桥梁。

可知，使用 OPC 可把通信程序与应用程序分开。通信程序由 PLC 厂家或专门软件公司提供，用于与 PLC 通信，作 OPC 的服务器。而应用程序由 PLC 用户编写，作为 OPC 的客户。两者再通过程序之间的数据交换，使 OPC 客户间接实现了对 PLC 监控与数据采集。

用于 PLC 的 OPC 服务器除了自身实现与 PLC 通信的功能外，与其他 OPC 服务器一样，也要有一组组接口（interface），并通过这些接口，为客户提供服务。

OPC 的服务软件多是要收费的。使用它也可不必弄清有关通信协议。

6. 组态软件通信

组态软件是专业公司在编程软件平台上开发的，介乎编程软件与应用软件之间“应用软件的半成品”。作为商业产品，组态软件一般都提供了友好的用户使用界面，还有变量库、图库、控件库以及脚本语言。同时，还都提供（收费或免费）种种与硬件通信的驱动程序。所以，有了它，用户可简便、灵活地设计画面，定义变量及调用驱动程序，基本上不用编写程序代码，或编写篇幅不大的脚本，就可组态成自己的应用软件。而实现的功能却与用编程软件开发的应用完全相当，而且一般还都具有更漂亮的画面。

此外，组态软件自身的固有优点：

易学习，学半个月、一个月就可上手，而 VB、VC 没有一年半载很难入门；

易开发，用组态软件开发应用，一个中等难度的一般工程，半个月就可以了，而用 VB、VC 少的一两个月，长的就更难说；

易维护，组态软件开发的应用，维护、修改很容易，而 VB、VC 开发的应用，换一个人去读懂代码都不易，改就更难。编程的人“跳槽”，往往使“老板”为难也与此有关；

界面好，组态软件是专业厂家作为商品提供的，界面都比较美观，所以，用它开发的应用画面都可做得比较美观；

接口多，组态软件接口多，上可接种种数据库、种种管理网络，如 ERP 系统等，下可接种种现场设备，可发挥承上启下的作用。

当然，从通信的角度讲，由于组态软件都提供有与 PLC 的驱动程序。所以，也不必了解有关通信协议也可实现与 PLC 通信。

1.6.4 互联网通信

1. 利用互联网通信

最成熟的通信是电子邮件，可发送、接收报文，还可添加附件。通信数据量可大到以兆计。只是这样的通信没有建立连接，通信不是很可靠的。为此，最好双方要有约定，要通过

应答确保数据的安全传送。

2. web 通信

有的 PLC 的以太网模块可内置 web（万维网）的网页，提供网址，作为服务器。计算机用户可使用浏览器阅读此网页，读取 PLC 数据，以至上传、下载文件。还可进行 PLC 的远程诊断及系统维护。

1.6.5　利用公网通信

这里用的公网主要指固定电话网、移动电话网及有线电视网络。

1. 固定电话通信

它主要用于通话，传送的是模拟信号。但随着调制解调技术的开发与应用，也允许数字信号在其上传输。这样，计算机、PLC 这样的数字系统利用它进行通信业就有了可能。

如 PLC 要与计算机通过串口用固定电话通信，首先双方都要安装有调制解调器。并且要先拨号，得到对方应答，叫通（建立连接）后，通信才可进行。一旦双方建立连接，固定电话对通信过程将是透明的，如同串口间直接连线，电话不存在一样。

固定电话通信在早期的远程数据采集的系统中，曾常用到它。此外，固定电话还是互联网的接入接口之一。所以，当使用互联网通信，它也是不可或缺的。

2. 移动电话通信

移动电话通信可使用发短信与 PLC（GSM）通信，也可使用 GPRS 与 PLC 通信。

使用 GSM 通信可以不建立连接，不占用线路，所以费用较低，很适合 PLC 把事件信息向计算机或其他 PLC 发送。但为了通信可靠，最好发去的信息能得到对方回应。这样的回应只要各方都运行了相关通信程序是不难实现的。

使用 GPRS（General Packet Radio Service）即通用分组无线业务通信。其 PLC 要先通过其串口与如同手机那样的 GPRS 模块相连。并通过 Windows 超级终端对该模块做好移动通信标示号（类似手机号）及允许访问它的计算机 IP 地址等设定。然后，PLC 上电、运行，通过移动通信的服务器接入移动通信网络（相当于手机上电后入网）。由于移动通信的服务器是与互联网也是相连的，这样，被这个 PLC 确认 IP 地址的计算机，只要也接入互联网，并运行相关应用程序，即可远程读写这个 PLC 数据，甚至控制 PLC 工作。

GPRS 的特点是：每个用户可同时占用多个无线信道，资源被有效利用，数据传输速率高达 160Kbit/s；允许用户在端到端分组转移模式下发送和接收数据，而不需要利用电路交换模式的网络资源，从而提供了一种高效、低成本的无线分组数据业务；特别适用于间断的、突发性的和频繁的、少量的数据传输，也适用于偶尔的大数据量传输；用户可永远在线，但收费不是按时间计算，而是按流量计，服务成本较低。

此外，由于移动电话技术的发展，目前已可利用它作为互联网的接入接口。如果 PLC 以太网模块也具备接入无线互联网能力，也可通过它利用互联网通信。

3. 有线电视网络

有线电视网络是基于光纤技术，传输速度很快。它的触角已深入到各个社区、工厂，是互联网很好接入接口。所以，使用它也可实现 PLC 与互联网对接，实现 PLC 与 PLC，或 PLC 与计算机之间的通信。

第 2 章　PLC 串口网络配置

关键词：RS-232C、RS-422A、RS-485、USB、DTE、DCE

PLC 串口网络指，各个站点均使用标准串口进行物理连接，链路层、应用层协议又较为简单的网络。标准串口，简称串口，指的是符合 EIA（Electronics Industries Association）标准的通信接口。

计算机、PLC 及现场设备多集成有这样的接口。利用这些标准串口，通过相应的通信介质，使计算机、PLC 及现场设备进行物理连接，进而实现数据通信，是最简单、最方便、最经济的 PLC 网络。同时，它也是最基本、最基础的 PLC 网络。因为对 PLC 网络而言，可以什么网络都没有，就是不能没有它。即使有别的网络可用以实际工作，但这些网络的设定多要通过它。

但是，串口网络毕竟通信速率低，通信数据量小，直接通信的距离短。它是面向字符的传输，同样传输量，所含的信息量也比面向“位”的传输要少，传输效率不高。因而，用它作为 PLC 网络的解决方案，只能算是低级的、基础的方案。而且随着现场总线的使用及其他 PLC 网络的进步，串口网络在实际系统的应用已逐渐被代替。

本章将讨论计算机及 PLC 的标准串口配置、功能及其设置。

2.1　计算机标准串口

关键词：RS-232C、RS-422A、RS-485、接口特性、DTE、DCE、调制解调器、握手、USB、IEEE1394

计算机标准串口有 RS-232C、RS-422A、RS-485，本节分别对其做介绍。此外，本节还将讨论 USB 等其他接口。

2.1.1　RS-232C 接口

RS-232C 接口是指合乎 RS-232C 标准的串行通信接口。RS-232 标准（协议）的全称是 EIA-RS-232 标准，是 1960 年，EIA（Electronic Industry Association），即美国电子工业协会制定的。RS（Recommended standard）代表推荐标准，232 是标准的标识号。以后又陆续发布了修订版本 RS-232A、RS-232B 和 RS-232C。目前广泛应用的是 RS-232C，为最新一次修改。

RS-232C 标准定义的是，数据终端设备 DTE（Data Terminal Equipment）和数据通信设备 DCE（Data Communication Equipment）之间串行二进制数据交换接口的技术标准。DTE 可以是计算机，也可以是 PLC 或现场设备，指需要的数据通信站点。DCE 是用以实现站点间通信的设备，如调制解调器（Modem）等。它的典型应用如图 2-1 所示。

从图 2-1 可知，有了 DCE 这个通信设备，两个 DTE（站点）可通过电话网络建立物理

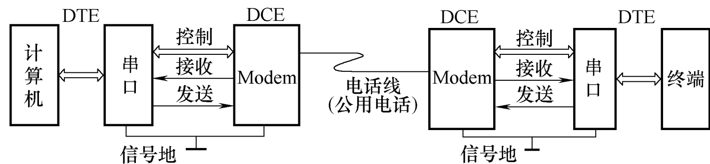


图 2-1　RS-232C 串口典型应用

连接，进而才可进行数据通信。

DCE 也还可以是无线调制解调制器。在各无线调制解调制器间，可通过无线电波或红外线传送信号，也可达到数据通信的目的。

当然，也可不用 DCE，两个 DTE 通过通信电缆直接连接。

1. RS-232C 接口特性

RS-232C 标准对串口规定有电气特性、机械特性、功能特性及规程特性，并对其多有所推荐。没有推荐的也有俗成约定。只是这个标准毕竟是美国的，而且年代又较久远，所以在使用时，还要注意到不同使用者对其理解与实施时的差异。

（1）电气特性

电气特性规定信号电平、电路连接方式、串行数据的传输格式、速率、距离以及与互连电缆相关的规则等。

RS-232C 标准规定，有两条数据、多条控制信号线及一条共用信号地线。适用于 1 对 1 全双工通信。

RS-232C 标准规定，信号为负逻辑。在数据线及控制线上，逻辑 1 为 −3 ~ −15V，逻辑 0 为 +3 ~ +15V。输入的逻辑电平是 +3 ~ +15V 和 −3 ~ −15V。输出为 +5 ~ +15V 和 −5 ~ −15V。输入与输出不同主要是考虑到抗干扰裕度。即 DTE 与 DCE 间允许有 2V 压降。

RS-232C 标准规定，数据按字符（节）为单位传送。每个字符（节）用起始位及使用相同的发送接收速率，保证收发同步。

（2）功能特性

功能特性规定了接口引脚功能和接线。当初，它规定了 21 条信号线，但在这 21 条中，常用的仅 9 条，也因此 9 针连接器很常用。这 9 针连接器引脚的信号线定义见表 2-1。

表 2-1　9 针 RS-232C 接口引脚定义

引脚号(9 针)	信号	方向	功　能
1	DCD	IN	数据载波检测
2	RxD	IN	接收数据
3	TxD	OUT	发送数据
4	DTR	OUT	数据终端装置(DTE)准备就绪
5	GND		信号公共参考地
6	DSR	IN	数据通信装置(DCE)准备就绪
7	RTS	OUT	请求传送
8	CTS	IN	清除传送
9	CI(RI)	IN	振铃指示

（3）机械特性

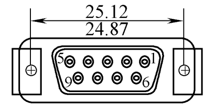


图 2-2　9 针接口简图

规定物理连接的插头和插座的几何尺寸、插针或插孔芯数及排列方式、锁定装置形式等。但 RS-232C 标准并未对机械接口做出严格规定。目前常用的 9 针 DB 连接器（插头、插座）简图如图 2-2 所示。

插针或插孔连接器的几何尺寸是相配合的，互成镜像对称。连接器的 DTE 端为针，DCE 端为孔，与它相接的为针。一般来说，作为 DTE 的计算机的连接器为针，而 PLC、现场设备，同样也是 DTE，但使用孔。

（4）规程特性

规定串口通信的实现过程或步骤。与是否通过 DCE 有关。以下是两个计算机通过 DCE（调制解调器 Modem）连接进行通信的具体步骤：

第一步，将计算机和 Modem 分别加电，计算机将“数据终端就绪”（Data Terminal Ready，DTR）信号线置为“ON”状态，而 Modem 则将“数据设备就绪”（Data Set Ready，DSR）信号线置为“ON”状态，此时 Modem 处于命令方式（空闲状态）。

第二步，计算机 A 通过“发送数据”（Transmit Data，TxD）信号线发出拨号命令给 Modem A，通知 Modem A 摘机并拨号。

第三步，Modem B 检测到振铃信号后，通过“振铃指示（Ring Indicator，RI）”信号线通知计算机 B 对呼叫进行应答。而计算机 B 通过“数据终端就绪（DTR）”信号线允许 Modem B 自动应答 Modem A 的拨号呼叫，即 Modem B 发出摘机信号（音频信号）。

第四步，当 Modem A 收到 Modem B 返回的应答音频信号后，随即向 Modem B 发送载波，而 ModemB 收到载波后，通过“载波检测”（Carrier Detection，CD）信号线通知计算机 B 线路接通，同时回应以自身的载波给 Modem A。而当 Modem B 检测到 Modem A 发出的载波后，它也通过载波检测 CD（Carrier Detection）信号线通知计算机 A 线路接通。此时计算机 A 和计算机 B 接通，Modem 进入联机状态（即数据方式），通信双方可以进入数据通信。

第五步，计算机 A 通过“发送数据”（TxD）信号线将数据发送给 Modem A，Modem A 将该二进制数据调制成一串不同频率的音频信号通过公用电话网发送给 Modem B，Modem B 则从音频信号中解调出原始数据并通过“接收数据”（Receive Data，RxD）信号线将数据送给计算机 B 上。而计算机 B 向计算机 A 发送数据的过程与此相同。计算机在发送数据过程中，要求“请求发送”（Request To Send，RTS）信号线为 ON 状态；而在接收数据过程中，要求“载波检测”（CD）信号线为“ON”状态。

第六步，计算机 A 通过将“请求发送”（RTS）信号线置为 OFF 状态以通知 Modem A 数据发送结束。Modem A 检测到 RTS 信号为 OFF 状态后，停止发送载波，并置“允许发送”（CTS）信号线为 OFF 状态以响应计算机 A。而 Modem B 检测不到载波后自动恢复到待机状态，并置“载波检测”（CD）信号线为 OFF 状态，通知计算机 B 不能接收数据。

第七步，计算机 A 置 DTR 信号线为 OFF 状态，通知 Modem A 拆线。Modem A 收到 DTR 的 OFF 信号后撤除与电话线的连接，并将 DSR 信号线置为 OFF 状态作为回答。

另外，在计算机发送数据到 Modem 的过程中，如果 Modem 的接收速度太慢，则 Modem 可以通过降下 CTS 信号通知计算机暂停发送数据。而且两个 Modem 建立载波连接后将继续保持载波连接，当载波消失或中断几十分之一秒后，连接被终止。

图 2-3 所示为计算机串口与 PLC 串口，通过 DCE（调制解调器，Modem）连接示意。

如果使用DCE是拨号Modem，也是要先拨号，要求建立连接；经对方回应确认，进而实际建立连接；然后才可通信。通信后还要挂机，断开连接。

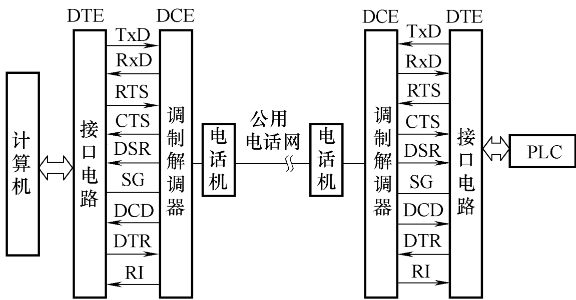


图2-3 计算机与PLC通过DCE连接示意

提示：这里的Modem是有线的。市场上还有无线Modem。它通过无线电波或红外线传输信号。它不仅与这里讲的RS-232C接口连接，也可将要介绍的RS-422/485接口连接。如果通信站点双方或各方都连接这样的Modem，则可在站点间实现无线信号传送。

必须注意的一点是，两个Modem在进行真正数据传输之前，必须首先交换如何向对方发送数据的信息，这一过程叫做交接过程。两个Modem必须就以下事项协调一致：传输速度、组成数据包的位数、包的起始位/停止位、奇偶校验以及半双工/全双工等。

如果计算机通过DCE连接与PLC连接并发起通信，则要把PLC方的Modem置为准备接收呼叫状态。办法是，把PLC方的Modem接于计算机串口，调Windows附件中的超级终端，在其窗口上键入以下3条命令：

atso =1 （设置准备接收状态）

at&wo （存于寄存器）

at&yo （上电时调寄存器）

这样，Modem接PLC，上电后，则它的AA指示灯亮。这表明PLC方Modem已作好接收呼叫的准备。这时，一旦计算机呼叫它，经一声振铃响，即响应，并强占电话线。

计算机方要发起通信，则要在用户程序中，执行与PLC方Modem通信的呼叫代码。也可通过超级终端键入呼叫代码。呼叫的代码是：

atdt + PLC方电话号码 + 回车

一旦呼叫成功，将返回相应信号，双方Modem的CD指示灯均亮。这时，计算机与PLC通信完成了通信连接。其间虽经过Modem、电话局，但将如同直接连线，即可通信。

当通信距离较近时，可不需要DCE。通信双方可以直接连接。有两种连接方式：一为有握手信号连接；另一为无握手信号连接。后者更常用。

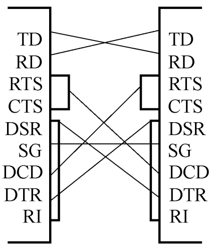


图2-4 RS-232C口有握手信号连接

有把握手信号连接称交叉环回接口连接，也称假Modem连接，较完整的连接如图2-4所示。

双方需用7条线，数据交换前要进行“握手”。“握手”成功才可交换数据。双方“握手”信号过程如下：

1）当甲方的DTE准备好，发出DTR信号，该信号直接连至乙方的RI（振铃信号）和DSR（数传机准备好）。即只要甲方准备好，乙方立即产生呼叫（RI）有效，并同时准备好（DSR）。尽管此时乙方并不存在DCE。

2）甲方的RTS和CTS相连，并与乙方的DCD互连。即一旦甲方请求发送（RTS），便立即得到允许（CTS），同时，使乙方的DCD有效，即检测到载波信号。

3）甲方的 TxD 与乙方的 RxD 相连，一发一收。

图 2-5 所示为零 Modem 方式的最简单连接（即三线连接），图中最上方的两条线是交叉连接。这样，把通信双方都当做数据终端设备看待，双方可发，也可收。通信双方的任何一方，只要请求发送 RTS 有效和数据终端准备好 DTR 有效，即能开始发送和接收。

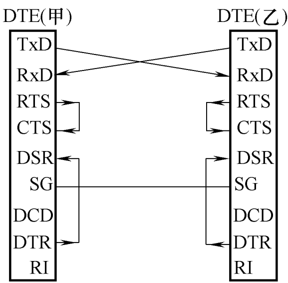


图 2-5　RS-232C 口无握手信号连接

2. RS-232C 的不足之处

RS-232C 接口信号电平值较高，易损坏接口电路的芯片。只能进行一对一的连接。不能实现与多个站点通信。使用一条共用信号地线，共地传输，易产生共模干扰，抗噪声干扰弱。所以，传输距离（电缆长度）是受限制的。当传输速率为 19200bit/s，误码率小于 4% 时，要求导线的电容值应小于 2500pF。对于普通导线，其电容值约为 170pF/m。所以，其最大传输距离可按下式计算：

$$允许距离\ L = 2500\text{pF}/(170\text{pF/m}) = 15\text{m}$$

当使用 9600bit/s，普通双绞屏蔽线时，距离可达 200ft。当使用 1200bit/s，普通双绞屏蔽线时，距离可达 3000ft。

2.1.2　RS-422A 接口

为了克服 RS-232C 标准的不足，于 1977 年底，EIA 颁布了新的接口标准。几经改进后出现了 RS-422A 标准。规定控制信号不用了。规定的信号电平降低为 ±6V（±2V 为过渡区域，仍为负逻辑）。规定发送器、接收器分别采用平衡发送器和差动接收器。这相当于差动直流放大器可消除零点漂移一样，消除共模干扰。所以，抗串扰能力大大增强。

图 2-6 所示为 RS-422A 四线接口电气原理图。除 4 条信号线，还有一条信号地线。数据线发送端（SDA、SDB）与对方的接收端（RDA、RDB）相连。各有其通道。无须握手直接可以进行双向数据交换。

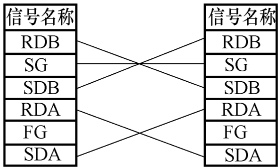


图 2-6　RS-422A 四线接口电气原理图

RS-422A 的接收器输入阻抗较高（4kΩ），发送器的驱动能力也比 RS-232C 大，所以它允许一个发送器可连接多到 10 个站点。但其中只有一个主站点（Master），其余为从站点（Salve）。而且从站点之间不能通信。

RS-422A 平衡双绞线的长度与传输速率成反比。最大传输距离为 4000ft（约 1219m），最大传输速率为 10Mbit/s。一般 100m 长的双绞线上所能获得的最大传输速率仅为 1Mbit/s。

RS-422A 连线时，在传输电缆的两个最远端，要接终端电阻，要求其阻值约等于传输电缆的特性阻抗。但距离较短、300m 以下，一般可不接。

2.1.3　RS-485 接口

RS-485 是从 RS-422A 基础上发展而来的。它的许多电气规定与 RS-422A 相仿。如都采用平衡传输方式、在传输线终端接终端电阻的要求也与 RS-422A 相同。但 RS-485 连线可用 4 线制，也可用 2 线制。

采用 4 线连接也只能有一个主（Master）站，其余为从站。从站之间也不能通信。但从站数可增加到 32 个。

RS-485 用的更多的是 2 线制，采用半双工方式。靠使能控制达到双向通信的目的。其接线如图 2-7 所示。在一个总线上，它可允许连接多达 128 个 RS-485 接口（站点）。而且站点间可实现相互通信。

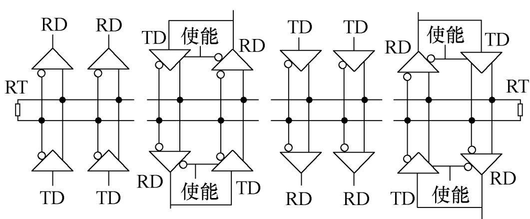


图 2-7　RS-485 接口连线

从图知，在 RS-485 中有一个“使能”端（该图未全画出），用于控制发送驱动器与传输线的切断与连接。那个站点要发送数据，则用“使能”端激活，而其他站点则只能接收数据。

RS-232C、RS-422A 及 RS-485 有关电气规定参见表 2-2。

表 2-2　RS-232C、RS-422A 及 RS-485 有关电气规定

规　　定		RS-232C	RS-422A	RS-485
工作方式		单端	差分	差分
站点数		1 收、1 发	1 发 10 收	1 发 32 收
最大传输电缆长度/ft		50	400	400
最大传输速率/bit/s		20K	10M	10M
最大驱动输出电压/V		+/-25	-0.25 ~ +6	-7 ~ +12
驱动器输出信号电平(负载最小值)/V	负载	+/-5 ~ +/-15	+/-2.0	+/-1.5
驱动器输出信号电平(空载最大值)/V	空载	+/-25	+/-6	+/-6
驱动器负载阻抗/Ω		3k ~ 7k	100	54
摆率(最大值)/V/μs		30	N/A	N/A
接收器输入电压范围/V		+/-15	-10 ~ +10	-7 ~ +12
接收器输入门限/mV		+/-3000	+/-200mV	+/-200mV
接收器输入电阻/Ω		3k ~ 7k	4k(最小)	≥12k
驱动器共模电压/V			-3 ~ +3	-1 ~ +3
接收器共模电压/V			-7 ~ +7	-7 ~ +12

提示：由于 RS-485 接口的优越的特性，有的 PLC 专用网络的物理层，如 Profibus、CC-Link 网，也是用 RS-485 串口标准。

计算机一般不配 RS-485 口，但工业 PC 多有配置。一般计算机要配备 485 口，也可通过插入通信板扩展。

PLC 的不少通信模块配用 RS-485 口。如和利时的 LM3108、3109 机。OMROM 的 CP1H 的内置串口板，西门子的 S7 机的 PPI、MPI、Profibus 网用的都是 RS-485 口。

提示：RS-232C、RS-422A 与 RS-485 标准只对接口的电气特性做出规定，而不涉及接插件、电缆或协议，在此基础上用户可以建立自己的高层通信协议。

2.1.4　USB 口

除了串口，用串行传输方式传送数据的，还有 USB（Universal Serial Bus）接口。是康

柏、微软、IBM、DEC 等公司为解决传统总线不足，于 1995 年推广的一种新型的接口标准。

目前使用的有两个版本，USB1.1、USB2.0。USB1.1 的最高数据传输率为 12Mbit/s。USB2.0 规范是由 USB1.1 规范演变而来的。它的传输速率达到了 480Mbit/s，足以满足大多数外设的速率要求。USB2.0 中的“增强主机控制器接口”（EHCI）定义了一个与 USB1.1 相兼容的架构。它可以用 USB2.0 的驱动程序驱动 USB1.1 设备。也就是说，所有支持 USB1.1 的设备都可以直接在 USB2.0 的接口上使用而不必担心兼容性问题，而且像 USB 线、插头等附件也都可以直接使用。

USB 连接线为设备还可提供最高 5V，500mA 的电力。USB 口的数据传输距离不大。超过 5m 不能通信。

USB 口可热插拔，其连接的外设可即插即用。此外，USB 接口还具有体积小、安装方便、高带宽、价位低、易于扩展、可连接数多台外设（最多可连接 127 台），以及可在线供电，不占系统资源，可错误检测与复原，节省能源等优点。所以 USB 接口已经成为计算机的标准接口之一。

USB 接口有 3 种类型。

TypeA：一般用于 PC；

TypeB：一般用于 USB 设备；

Mini-USB：一般用于数码相机、数码摄像机、测量仪器以及移动硬盘等。

配备 USB 口的两台计算机还可通过 USBLink100 专用电缆非常方便地实现双机连网。该电缆提供有驱动程序（SMART-Linq 程序）。安装好驱动程序（安装程序会在桌面上建立一个 PC-Linq 的快捷菜单），做好计算机 BIOS 正确设定，重新启动计算机，即可连网。这时，两个计算机各运行 PC-Linq 程序，即可看到，类似 Windows 下的“资源管理器”一样 PC-Linq 窗口，将分别显示两个计算机的资源。在这个窗口上，同样支持复制、粘贴、创建、删除和直接拖曳等，与“资源管理器”的功能相同。不同只是“资源管理器”只能管理本地计算机上的资源，而 PC-Linq 窗口却能同时管理两台计算机上的资源。

除以上所介绍的常用功能外，在 PC-Linq 窗口中还可以共享另一台计算机的软驱、光驱、文件和打印机等资源。其中，共享对方的软驱、光驱和打印机时，无论从操作方式还是从速度上看，与在本地计算机上几乎没有什么区别；如果对方计算机上的应用程序没有严格的连接要求，一般都能通过调用在本地计算机上运行。其他的如 WAV、MP3 及一些文本文件都可以直接在本地计算机上顺利调用。

提示：在从计算机上拔掉 USBLink 电缆之前一定要先关闭本地的 PC-Linq 窗口，否则会因中断连接而产生蓝屏，甚至是死机。

正是 USB 口有这么多的优点，最新出厂的 PLC，如 OMRON 的 CP1H、CP1E 机及 CJ2 机等，也配置有这个接口，可使用它通过厂家所提供的编程软件，与计算机直接通信。而且，对于 CJ2H-CPU6@-EIP 或 CJ2M-CPU3@，还可通过 USB 端口访问 EtherNet/IP 网络中的 PLC。

最后要指出的是，在美国旧金山举行的 2007 秋季 IDF 上，由英特尔、微软、惠普、NEC、NXP 半导体和德州仪器六家行业巨头组成的 USB3.0 促进者社团（USB3.0 Promoter Group）发布了超高速 USB（Super Speed Universal Serial Bus）互联规格，即 USB3.0。该社团宣布，其传输速率可达 2.0 版的 10 倍，将广泛应用于 PC、消费电子和移动设备领域。而

NEC 公司已宣布将发布首款支持 USB3.0 标准的控制芯片 μPD720200 和支持 PCI-E2.0 总线的扩展卡。这意味着 USB 口将有更长足的进步。

2.1.5　IEEE1394 口

IEEE1394 口的前身叫 Firewire（火线），是 1986 年由苹果电脑公司针对高速数据传输所开发的一种数据传输接口，并于 1995 年获得美国电机电子工程师协会认可，成为正式标准。现在看到的 IEEE1394、Firewire 和 i. LINK 其实指的都是这个标准。

通常，在个人计算机领域将它称为 IEEE1394，在电子消费品领域，则更多的将它称为 i. LINK，而对于苹果机则仍以最早的 Firewire 称之。

IEEE1394 也是一种高效的串行接口标准，功能强大而且性能稳定，支持热拔插和即插即用。IEEE1394 可以在一个端口上连接多达 63 个设备，设备间采用树形或菊花链拓扑结构。

IEEE1394 标准定义了两种总线模式，即：Backplane 模式和 Cable 模式。其中 Backplane 模式支持 12.5、25、50Mbit/s 的传输速率；Cable 模式支持 100、200、400Mbit/s 的传输速率。目前最新的 IEEE1394b 标准能达到 800Mbit/s 的传输速率。

IEEE1394 是横跨计算机及家电产品平台的一种通用界面，适用于大多数需要高速数据传输的产品，如高速外置式硬盘、CD-ROM、DVD-ROM、扫描仪、打印机、数码相机、摄影机等。

IEEE1394 分为有供电功能的 6 针 A 型接口和无供电功能的 4 针 B 型接口，A 型接口可以通过转接线兼容 B 型，但是 B 型转换成 A 型后则没有供电的能力。6 针的 A 型接口在 Apple 的电脑和周边设备上使用很广，而在消费类电子产品以及计算机上多半都是采用简化过的 4 针 B 型接口，需要配备单独的电源适配器。

相比 USB1.1，1394a 接口在速度上占据了很大的优势。而当 USB2.0 推出后，1394a 接口在速度上的优势就不再那么明显了。同时现在绝大多数主流的计算机并没有配置 1394 接口。但可以通过插接 IEEE1394 扩展卡的方式获得此接口。而 PLC 则都还没有配置这样接口的机型。

IEEE1394 接口工作速度虽快，但传输的距离很短，最长仅 4m 左右。

2.1.6　通信口转换

从以上介绍可知，标准通信接口种类很多。不同类型的接口，其电气、机械及工作特性也不相同。所以，要实现通信，两个设备的通信接口类型不同，其间的连接、通信是无法实现的。

计算机及需要通信的设备类型、品牌、规格很多，生产的厂家也很多，要求所有这些产品都使用同一种通信接口，当然是不可能的。更何况通信接口技术还在不断发展呢！所以，为实现不同特性的接口的计算机及设备能够互联、互通，则必须使用接口转换器，或称适配器，如 USB 口转换成 RS-232C 的适配器，RS-232 口转换成 RS-422A、485 的转换器等。用它后，可对其中的一方接口进行转换。把其中一方的通信接口转换与另一方的相同，双方的连接、通信则有可能了。

特别当今，有的电脑，特别是“笔记本电脑”，已不配置串行接口，而只配置 USB 口。为了与配备 RS-232C、RS-485/422 口的设备连接、通信，就必须使用 USB 口到 RS-232C、

RS-485/422 口的转换器，以便它转换为 RS-232C 口、RS-485/422 才可。

再就是，由于计算机要接入的通信设备不断增多，有时可能出现通信接口不够使用的情况。这时，计算机还可配置如以太网卡那样的串行接口卡。配置后，其上就有相应标准接口。一个板卡提供几个、十几个接口的都有。

可知，有了转换器、板卡，计算机的标准接口可以转换，也可以增多。而且现在，开发、生产这样转换器、板卡的厂家很多。市场上这类产品也很多，价格也较为低廉，这就为计算机通过标准接口，实现与多种设备连接、通信提供了很大方便。

要指出的是，把 USB 口转换为标准串口只是“虚拟串口”。可能有的以前在传统 RS-232C 口上运行的软件，使用它却不能够正常运行。所谓“传统 RS-232C 口”是指从 PC 的主板或者总线，比如台式机的 PCI 或者 ISA 总线、笔记本的 PCMCIA 总线上扩展出来的 RS-232C 口。这是因为 USB 与 PCI 之类的并行总线有本质的区别。USB 口没有分配固定的总线 I/O 地址，也没有固定的中断号，它的地址是通过软件来虚拟的。而传统的 RS-232C 口有固定的 I/O 地址以及中断号。这就是某些通信软件在传统 RS-232C 口可以运行，而在 USB 到串口转换器的 RS-232C 口上不能够运行的原因。如果通信软件内有直接 I/O 读写语句，那么肯定无法在 USB/串口转换器的串口上运行。另外还有一个原因就是对 RTS/CTS、DTR/DSR 这些握手信号的操作，即使是通过虚拟读写不是通过直接 I/O 读写来操作这些握手信号，但由于 USB/串口转换器对这些握手信号的虚拟读写过程的初始化往往比较耗时，所以容易导致握手信号读写失败。

除了转换器，还有标准串口的“增强器”。用它可提高标准接口的通信能力，如增大通信距离，增强防干扰或抗雷击能力。这类“增强器”名称不一，或称适配器，或称收发器，或称串口泵。如 RS-232C 接口，原来最大传输距离只有 15m、波特率最高只有 19200bit/s，而经使用某厂家生产的串口泵“增强”，其传输最大距离可达 2km，波特率也可达 57600bit/s。这些增强技术的奥秘是，将 RS-232C 接口数据传送方式转换成浮地隔离双端平衡传输。同时，采用了光隔离，使得串口与设备之间没有电接触，只有光传送，大大地提高了系统的抗干扰能力，内置的抗雷击电路也可确保系统的安全。

串口连接媒体本来是使用双绞线，也可用适配器进行变换，改用光纤。很多 PLC 厂家，如 OMRON 就生产有这类适配器。使用这类适配器后，设备间用光纤连网、通信，不仅可增大网络站点间的距离、避免雷击、提高保密性，同时也可提高传输速率。有的产品还介绍说，经使用它的适配器产品变换后，传输距离可扩大到 20km。

再就是还有种种传输“中继器”。它可把收到的已减弱信号放大，放大后再向前传送。所以也是接口通信能力的“增强”。特别在使用 RS-485 时，在站点间增加多个中继器，可大大增加数据的传输距离。同时，还能增多网络站点的配置。

此外，目前，不仅有各种标准接口之间相互转换及增强的适配器，而且，还有把标准串口或 USB 口转换成以太网的适配器、连接移动通信的适配器。用它，也可通过标准串口或 USB 口接入以太网、移动通信网络。这样，站点间的数据交换及相互操作也可通过互联网、移动通信实现。

其实，在某种意义上讲 Modem 也可看成这样的转换器。有有线 Modem，还有无线 Modem。有线 Modem 可使两个站点通过拨号、应答，通过电话网络实现连接。而连接后这个电话网络对两个站点将是“透明”的，其间通信如同直接连线一样，而通信距离却随着电话

系统而无限增大。无线 Modem 信号有电磁波传送的，还有红外线传送的。前者要使用专用频率，距离可长可短，视生成信号的功率而定。后者距离较短，两个站点要处在相互视野顾及之内。小功率的电磁波及红外信号传送很适合用于移动站点与固定站点之间的通信。在立体仓库中用得很多。

2.1.7　串口设定

使用串口还要做好设定，也就是要确定它的波特率、帧格式及校验处理。波特率控制数据发送与接收速率，只有通信双方传输速率相等，所发送的数据才能被正确接收。帧格式是指起始位、数据位及停止位的分配。常用的是 1 位起始位，7 或 8 位数据位，1 或 2 位停止位。校验有奇或偶校验，也可设为不用校验。帧格式及校验处理通信双方也要设定一致。注意，如果传输的为十六进制数，而不是 ASCII 码，则必须用 8 位数据位。

此外，还有数据流的控制。因为接收方在收到数据后，总是要进行处理的。如果接收方处理速度较慢，也有可能未把所接收的数据处理完毕，接收缓冲区还未清空，发送方又把数据发来。这样，就要造成数据丢失。这当然是不允许的。流控制就是接收方通过控制信号通知发送方是否发送或停止发送数据。

流控制有两种办法：硬件流控制及软件流控制。

硬件流控制：硬件流控制常用的有 RTS/CTS 流控制和 DTR/DSR（数据终端就绪/数据设置就绪）流控制。为此，必须将相应的电缆线连上。在编程时，要根据接收端缓冲区大小设置一个高位标志（可为缓冲区大小的 75%）和一个低位标志（可为缓冲区大小的 25%），当缓冲区内数据量达到高位时，在接收端将 CTS 置逻辑 0，当发送端的程序检测到 CTS 为逻辑 0 后，就停止发送数据。当接收端缓冲区的数据量低于低位时，再将 CTS 置逻辑 1。这时，发送端的程序检测到 CTS 为逻辑 1 后，又继续发送数据。

软件流控制：由于有的串口不使用控制信号线，流控制可用软件流实现。常用方法是：当接收端的输入缓冲区内数据量超过设定的高位时，就向数据发送端回应 X OFF 字符（十进制 ASCII 码值 19），而发送端接收到“X OFF”字符后，就停止发送数据。当接收端的输入缓冲区内数据量低于设定的低位时，就向数据发送端回应“X ON”字符（十进制的 ASCII 码值 17），而发送端接收到“X ON”字符后，继续发送数据。

应该注意，若传输的是二进制数据，标志字符也有可能在数据流中出现而引起误操作，这是软件流控制的缺陷，而硬件流控制不会有这个问题。

串口的设定多数是用软件在串口初始化时实现。有的设备也可使用硬件开关选定。

此外，对 PLC 串口，由于功能的增加，其设定的选项也相应增多。除了选定通信参数，还要选定所使用的功能及相关协议。

2.2　LM 机串口网络

关键词：自由协议通信、Modbus RTU 协议通信、调用设定功能块

2.2.1　LM 机串口配置

LM PLC，在 CPU 模块上，最少配置有一个串口（RS-232C）。点数多的机型，如

LM3109，除了配置有 RS-232C 口，还配置有 RS-485 口。

1. RS-232C 串行通信接口

在和利时 LM 系列 PLC 的 CPU 模块左侧，提供有 9 针 RS-232C 串口，如图 2-8 所示。表 2-3 为它的 RS-232C 口的接线定义。表 2-4 为它的 RS-232C 口的参数配置。

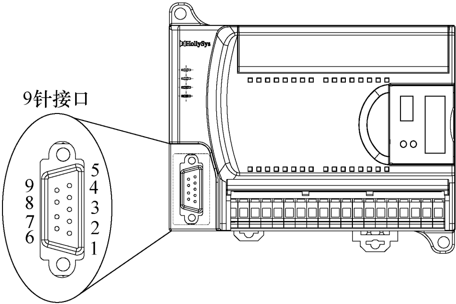


图 2-8 LM 机 RS-232C 口

表 2-3 LM 机 RS-232C 口接线定义

连接针号	定义	连接针号	定义
1	—	2	RXD
3	TXD	4	—
5	GND	6	—
7	—	8	—
9	—		

表 2-4 LM 机 RS-232C 口参数配置

项　目	参　数
物理接口	RS 232
通信速率	300 ~ 38400bit/s
通信协议	自由协议 Modbus RTU 协议 专有协议

2. LM 机 RS 485 串行通信接口

LM 机的 LM3108 和 LM3109CPU 模块，其左侧位置，除了配置有 RS-232C 口（Port1），还有 Port0，是标准 RS-485 串口，如图 2-9 所示。表 2-5 为它的 RS-485 通信口接线定义。表 2-6 为它的 RS-485 口的参数配置。

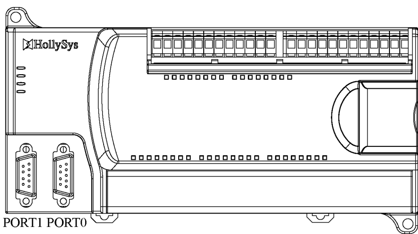


图 2-9 LM 机左侧位置的两个通信接口

表 2-5 LM 机 RS-485 通信口接线定义

连接针号	定义	连接针号	定义
1	—	2	—
3	B(+)	4	—
5	—	6	—
7	—	8	A(-)
9	—		

表 2-6 LM 机 RS-485 口的参数配置

项　目	参　数
物理接口	RS 485
通信速率	300 ~ 38400bit/s
通信协议	自由协议 Modbus RTU 协议

提示：LM 机还有 RS-485 通信模块，也可用于做通信接口配置。同时还有中继器，可用以增大通信距离。

2.2.2　LM 机串口功能

1. 利用 PowerPro 软件对 PLC 编程及监控

可以利用此接口，通过编程电缆，与计算机的 RS-232C 串口连接，可在 PowerPro 软件的平台上，实现 PLC 程序下装及测试程序；

当 PLC 面板开关处运行状态时，可远程操作 PLC，使其停止运行或进入运行；可诊断 PLC 状态，查找其故障履历；可监控 PLC 工作，包括回路监视，变量数值监视及更改；可用类似“组态软件”的方法，建立视图，用图形或数表的画面，对 PLC 控制系统实施监控。

2. 自由协议通信

可按需要，执行含有 COMM_SEND（发送，用于 RS-232C 口）、COMM2_SEND（发送，用于 RS-485 口），COMM_RECIEVE（接收，用于 RS-232C 口）及 COMM2_RECIEVE（接收，用于 RS-485 口）功能块的程序，利用 LEC-G3PLC 的 M 存储区，实现与通信对方交换数据，只是通信对方也必须执行相应程序。

3. Modbus 协议通信

Modbus 协议是 MODBUS 公司开发的主从站间的通信协议，通信口使用 RS-485 或 RS-232C。使用 RS-232C 只能是一对一链接。使用 RS-485 口，一个主站最多可接 32 个从站。

应答方式是主站向某个从站（地址可以是 1～247）发出命令，然后等待从站的应答；从站接到主站命令后执行命令，并将执行结果向主站应答，然后等待下一个命令。

广播方式是主站向所有从站发送命令（从站地址设为 0），不需要等待从站应答；从站接到广播命令后，执行命令，也不向主站应答。

LM 机与计算机、其他 PLC 及现场设备可利用此串口 Modbus 协议通信。通信时计算机、其他 PLC 及现场设备为主站，LM 机为从站。通信由计算机、其他 PLC 及现场设备发起，LM 机只是应答。而且，这个应答是系统完成的。但是 LM 机也应先运行初始化设定程序。

2.2.3　LM 机串口设置

LM 的串口参数设置的方法是，运行含有调用设定功能块初始化程序。如 RS-232C 口，则调用 Set_COMM_PRMT 功能块；如 RS-485 口，则调用 Set_COMM2_PRMT 功能块。

要使用 ModbusRTU 协议，则需要设定从站地址。这时要调用地址设定功能块，即 SET_LOCAL_ADDRESS。如要了解现有的从站地址，则可调用 GET_LOCAL_ADDRESS 功能块。

2.2.4　LM 机串口连网配置实例

1. 针对城市热网远程监控的 PLC 解决方案

用于对分布不同地理位置的，冬季供热用换热站的温度、压力、流量和液位等参数集中监控。同时，调节热电厂运行工况，保证冬季整个供暖的稳定运行。

具体解决方案是：在各换热站安装 PLC，进行参数采集、设备控制。而这些 PLC 又通过 GPRS 网络与调度中心控制计算机建立可靠、稳定的通信，以便在调度中心可对现场所有换热站完成监控。

该方案由 3 部分组成：现场换热站 PLC 控制部分、GPRS 数据传输部分和调度室数据中心。

PLC 在各换热站完成以下功能：现场温度、压力、流量、液位信号的采集；现场各调节阀的控制；现场电动机、变频器的控制及运行监视；监视控制、报警、历史曲线显示等功能。

在换热站中，用触摸屏进行人机交互，控制各种设备运行。对于现场调节阀及各种电机的控制，设计了就地控制、触摸屏控制和远程调度中心控制 3 种方式。

该方案具备非常好的抗干扰性（尤其是在城市中）和数据传输安全性，并在沈阳皇姑热电有限公司皇姑热网监控中得到实际应用，运行状况良好。调度人员可对全区 26 个使用 HOLLIAS—PLC 控制的换热站中任一设备进行远程控制，并监视所有工艺运行参数。同时，将所有工艺参数通过网关机，还可送到 MIS 网中进一步进行数据分析。这不仅提高了工厂的效率和效益，对于提高整个热网的运行水平也起到了重要作用。

2. 和利时 PLC 在无线数据采集系统中的应用

本系统分下位机、上位机两部分。下位机采用多个和利时公司的 PLC。分别对油田的 5 个计量站、2 个阀门组站进行数据采集及部分控制。计量站中的 PLC 通过 RS-485 通信口与一台智能质量流量计通信，读取流量计中的 16 个计量数据。PLC 还执行计量器间内三相分离器的压力调节和液位控制。此外，阀门组站内为 10 口井的计量阀组，也配有 PLC 的 CPU 模块和若干 I/O 模块。所有下位的 PLC 除执行控制任务外，还用其上的 RS-232C 通信口，通过无线 Modem、数据传送电台，与上位机通信。

上位机也称中心站，为普通计算机。运行和利时公司的 Focsoft3.0 软件。通过数据传送电台与下位 PLC 通信。在 Focsoft3.0 中定义一个轮询标签。每当系统对轮询标签采样时，Focsoft 自动启动操作电台，发出一个带站号的轮询指令。1～7#RTU 站均可以收到该指令。但只有自身站号符合轮询指令中站号的 PLC 才会应答。应答时，它将预先存储在寄存器中的数据上传。计算机收到数据后，向 PLC 发出确认信息，表明本次通信结束，并把数据存入相应的标签。当中心站有数据下传时，操作原理基本相同。PLC 将接收到的下传数据存入寄存器，供控制程序调用。轮询周期通过设定轮询标签的采样频率确定。如果某次通信因故没有成功，中心站会发出报警，直到下次通信恢复后报警结束。

本系统已在新疆塔里木油田桑塔木作业区范围内分布的油井中使用，运行稳定。中心站与 RTU 站间最远距离 13km，只要几分钟就可以准确地完成数据采集，实现了计量自动化、远程化。

2.3　OMRON PLC 串口网络

关键词：集成串口、外设口、串口内插板、模块式串口单元、上位链接、PLC Link、NT 链接、协议宏

2.3.1　OMRON PLC 串口配置

OMRON PLC 串口有 3 种配置方式。

1. 集成串口、外设口、USB 口

在 CPU 模块上，集成有外设口、RS-232C 口，有的还有 RS-422A 口、USB 口。图 2-10 所示为 CP1H 机面板及 USB 口。用它与计算机 USB 口连接，再使用 OMRON 编程软件，可

实现计算机对 PLC 的程序上下载、调试、PLC 系统设置及计算机监控。还有新机型 CP1E，其 CPU 仅集成 USB 口，可与计算机的 USB 连接，用以编程。

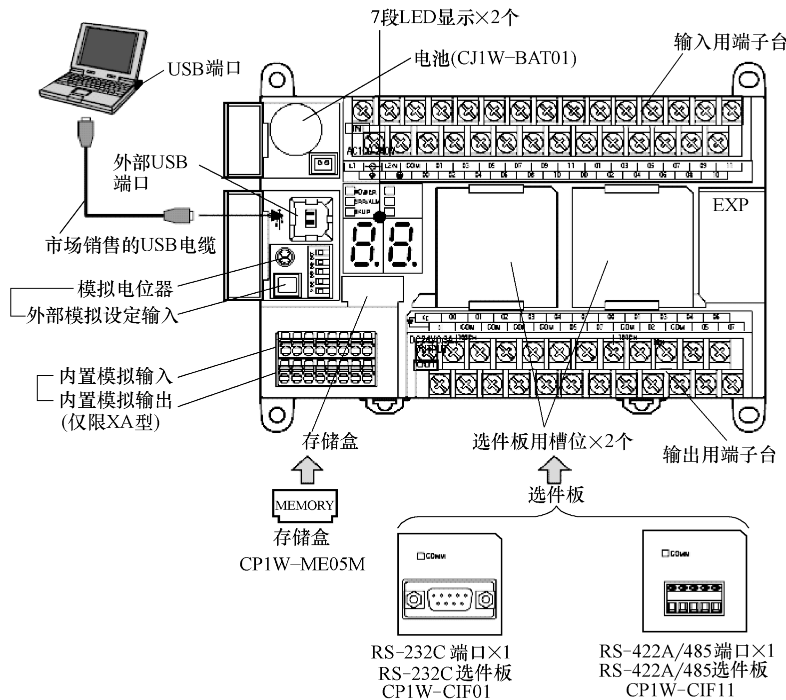


图 2-10　CP1H 机面板及 USB 口

图 2-11 为 OMRON 公司 CPM2A CPU30 模块的平面图。它有 30 个 I/O 点，有外设口，也有 RS-232C 口。外设口，用以连接手持（或图形）编程器，对 PLC 做手工编程。这个外设口若用适配器做了转换，也可成为标准串口（RS-232C 或 RS-422A、485），以实现串口通信功能。

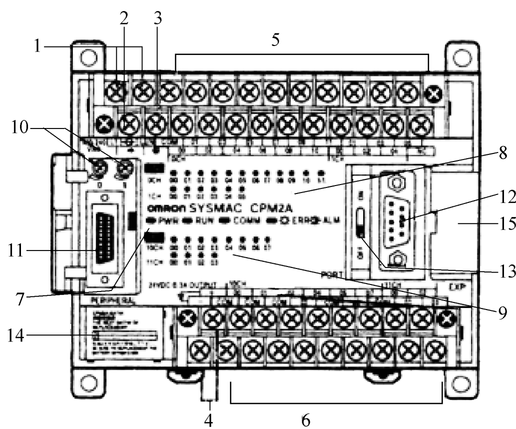
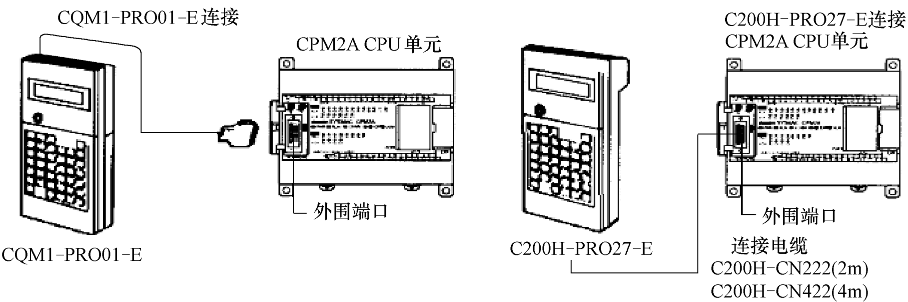


图 2-11　CPM2A CPU30 平面图

1—电源输入端子　2—功能接地端子　3—保护接地端子　4—24V 供电端子　5—输入端子　6—输出端子　7—状态指示灯　8—输入指示灯　9—输出指示灯　10—模拟设定电位器　11—外设端口　12—RS-232C 端口　13—通信设定开关　14—电池舱　15—扩展电缆接口

图 2-12 所示为外设口与简易编程器相连的情况。图 2-13 所示为外设口经过适配器转换与计算机相连的情况。图 2-14 所示为 RS-232C 口与计算机相连的情况。

CPM2A CPU 单元可通过标准的C200H−CN222(2m)或C200H−CN422(4m)连接电缆与C200H−PRO27−E编程器连接。CPM2A CPU 单元也可与CQM1−PRO01−E 连接。CQM1−PRO01−E 附带有A2m连接电缆



将编程器连接到CPU单元的外围端口，编程器不可接到RS−232C端口。PC在编程器方式下会自动地与编程器通信，而不管CPU单元的通信开关上所选择的通信方式

图 2-12　外设口与简易编程器相连

外围端口的连接
一台个人计算机可通过CQM1−CIF01或CPM1−CIF01 RS−232C适配器与CPU单元的外围端口连接。

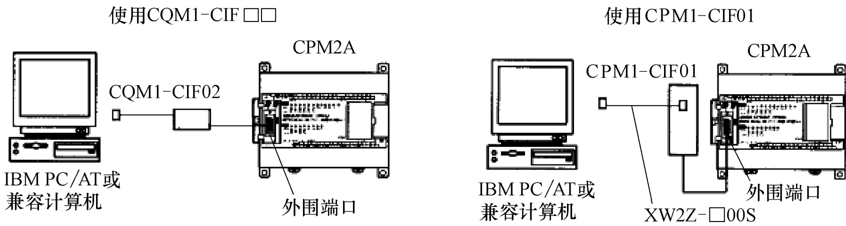


图 2-13　外设口经过适配器转换与计算机相连

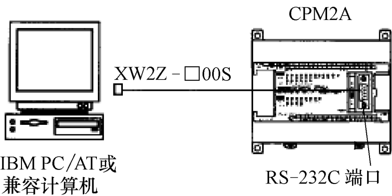


图 2-14　通过 RS-232C 口与计算机相连

2. 串口内插板

如图 2-15 所示，在 CPU 单元上，有两个串口选件槽位（1 或 2）。可供用户安装所选配的串口内插板。CP1H 机有 RS-232C、RS-422A/485 内插板。图 2-15 所示为 RS-232C 内插板。表 2-7 为 RS-232C 口连接器引脚信号分配。

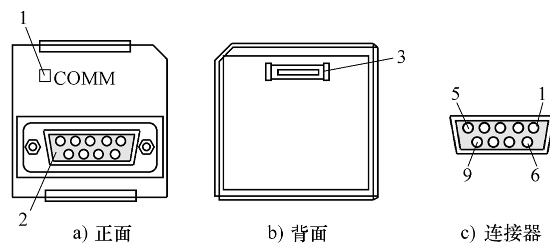


图2-15　RS-232C内插板

1—通信状态指示灯　2—RS-232C连接器　3—连接CPU连接器

表2-7　RS-232C口连接器引脚信号分配

引脚编号	信号略称	信号名称	信号方向
1	FG	帧用接地	—
2	SD(TXD)	发送数据	输出
3	RD(RXD)	接收数据	输入
4	RS(RTS)	发送请求	输出
5	CS(CTS)	清除发送	输入
6	5V	电源	—
7	DR(DSR)	数传机就绪	输入
8	ER(DTR)	终端设备就绪	输出
9	SG(0V)	信号用接地	—
连接金属	FG	帧接地	—

图2-16所示为RS-422A/485选件板。RS-422A/485选件板可在RS-422A与485件选择，选用表2-8为RS-422A/485口模式选择开关连接器引脚信号分配。

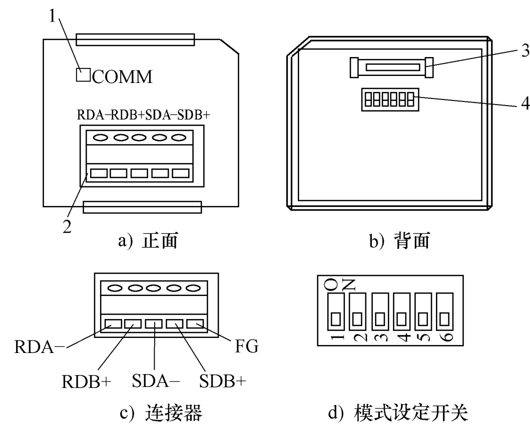


图2-16　RS-422A/485选件板

1—通信状态指示灯　2—RS-422A/485连接端子　3—连接CPU连接器　4—模式设定开关

3. 模块式串口单元

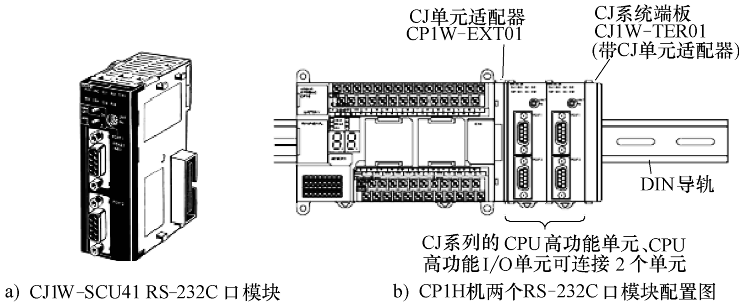
模块式标准串口的单元较多，如早期的C200H机Host-Link单元。再如CJ机也有此模块，如图2-17a所示，每个模块配置有两个串口。CJ1机除了CPU上集成有RS-232C口，还

表 2-8　RS—422A/485 模式选择开关连接器引脚信号分配

引脚 No.	设定内容		
1	ON	有(两端)	终端电阻有无的选择
	OFF	无	
2	ON	2 线式	2 线式/4 线式的选择①
	OFF	4 线式	
3	ON	2 线式	2 线式/4 线式的选择①
	OFF	4 线式	
4	—	—	空置
5	ON	有 RS 控制	选择 RD 的 RS 控制的有无②
	OFF	无 RS 控制(平时接收)	
6	ON	有 RS 控制	选择 SD 的 RS 控制的有无③
	OFF	无 RS 控制(平时发送)	

① 引脚 No. 2 及 3 请都设定为 ON（2 线式）或 OFF（4 线式）。
② 在需要禁止回送的情况下，将引脚 No. 5 设定为［有 RS 控制］(ON)。
③ 用 4 线式布线进行 1∶N 连接时，在连接到 N 侧的设备的情况下，将引脚 No. 6 设定为［有 RS 控制］(ON)。
在 2 线式布线进行连接的情况下，将引脚 No. 6 设定为［有 RS 控制］(ON)。

可配置多达 16 个串口单元、可增加 32 个串口。CP1H 为箱体式 PLC，但它也可扩展配置两个模块式串口单元，如图 2-17b 所示。



a) CJ1W-SCU41 RS-232C 口模块　　b) CP1H机两个RS-232C 口模块配置图

图 2-17　模块式串口单元

OMRON PLC 串口连网使用的介质多为双绞线。如使用 RS-232C 口，则站点间的距离不能超过 15m。如果使用 RS-422A 口，可增大到 400m 或更大。有的也可使用光纤，站点间距可增加到 1000m，或更大。只是使用光纤时，要选用可连接光纤的串口单元，同时，在计算机方还要使用相应的适配器，以进行电与光信号相互转换。

OMRON PLC 串口连网不提供中继器。但也可使用第三方的产品实现中继，以增大通信距离。但是，如果要求的距离在几公里或更大，则要另想办法。常用的有两个办法：一是通过调制解调器（Modem），利用电话网，实现通信；二是利用无线 Modem，通过专用无线电台或商用移动通信网络实现连网、通信。

提示：OMRON PLC 串口功能与 PLC 的型号、串口的类别及版本有关。一般讲新型号、新类别、新版本的功能更强。配置与使用时要弄清其功能是否合乎需要。

2.3.2　OMRON PLC 串口功能

不同机型串口功能不完全相同。高档机、新型机功能较多。除了上述用于系统设置、编程、上下程序、监控外，还有如下功能：

1. 上位链接

可利用串口，进行上位链接（HostLink），实现计算机对 PLC 的编程、管理及监控。此外，还有 ToolBus 功能与上位链接功能基本相似。但通信速率稍高。只有 CS 型及其后续机才有此功能。而且只能用 OMRON 编程软件才能通信。

上位链接可以是一台计算机与一台 PLC 进行 1∶1 链接，组成最简单的信息网。这时用的是 RS-232C 口，图 2-18 所示的即为此配置。

图 2-19 所示为计算机 RS-232C 口与 CP1H 机的 RS-232C 通信板的接线图。要注意的是，即使同为 OMRON PLC 的 RS-232C 口，其接口定义有可能与此不同。

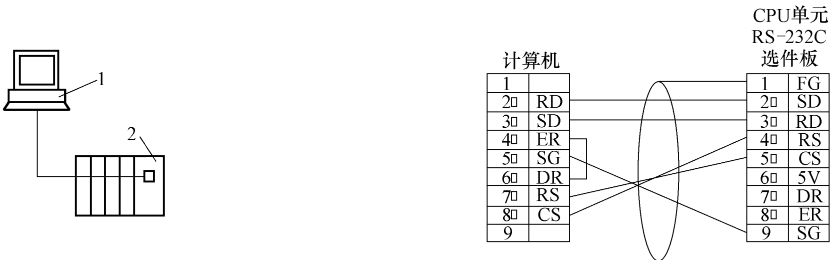


图 2-18　1∶1 信息网
1—计算机　2—PLC

图 2-19　计算机 RS-232C 口与 CP1H 机的 RS-232C 通信板接线图

除了 1∶1 链接，还可进行 1∶N、或 N∶1 或 N∶N 连网，组成较为复杂的信息网。图 2-20 所示为这些连网的配置图。这里的 N 可达 32 台。

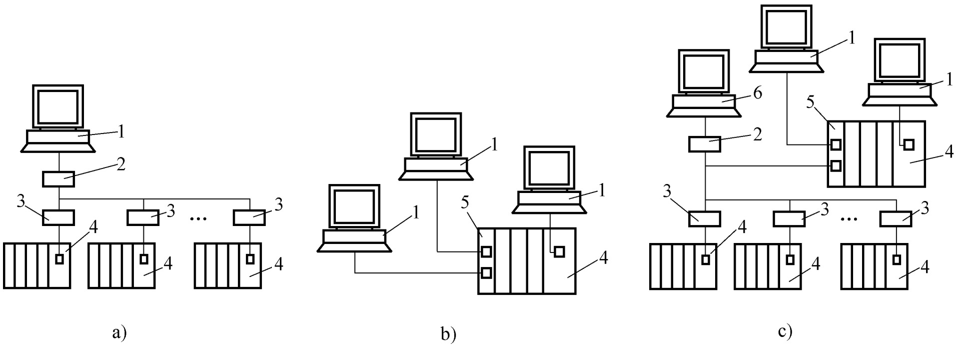


图 2-20　1∶N、或 N∶1 或 N∶N 连网配置

图 2-20a 为一台计算机与多台 PLC 连网。图中 1 为计算机，2 为 RS-232C 到 RS-422A 转换器。3 为分叉接线器。4 为 PLC 的配置有 RS-422A 口的 CPU 单元。

图 2-20b 为 3 台计算机与 1 台 PLC 连网。图中 1、4 同图 2-20a。5 为串口通信模块。要用其上的两个 RS-232C 口，分别与两台计算机相连。这样，可实现处于不同位置的 3 台计算机同时监控一台 PLC。

图2-20c为3台计算机与4台PLC连网。图中1、2、3、4同图2-20a。6为计算机。5为串口通信模块。要用其上的一个RS-232C口、一个RS-422A口，分别与两台计算机相连。这样，可实现处于不同位置的3台计算机同时监控一台PLC。同时，计算机6还可监控其他3台PLC。但对多台PLC监控要使用RS-422A接口。

使用HostLink连网功能，计算机可通过OMRON编程软件与PLC通信。也可由用户按OMRON的HostLink等协议自编应用程序与PLC通信。而且通信多是由计算机发起，PLC响应。但对C系列机，通信也可由PLC发送通信命令发起，让计算机响应。而对CJ/CS系列机，虽不能用C模式通信命令发起通信。但它可用FINS模式通信命令发起通信，让计算机响应。此外，使用FINS命令，还可跨网络、通过网桥设定好路由，实现计算机与PLC或PLC与PLC通信。

2. PLC Link

利用串口，可实现PLC间的数据区链接通信。PLC Link原是OMRON的一种PLC间通信网络。入网的PLC都要使用PLC Link模块，并用双绞线连接、连网。但它的新型别PLC，利用串口也可实现这种连网。PLC Link链接通信机理已在本书1.6节做过介绍。

PLC链接通信区的大小及可参与链接的PLC数量与PLC的型别有关。要按有关说明书要求配置。如CP1H机，可实现1∶1链接，也可实现1∶N（最大为8台）链接。

图2-21所示为CP1H机的1∶1PLC链接，实现两台PLC之间的数据交换。可以是CP1H机间链接（见图2-21a），也可CP1H机与CJ1M机链接（见图2-21b）。

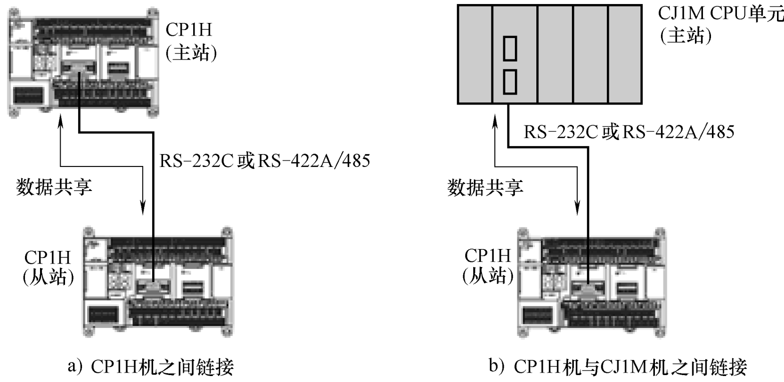


图2-21　1∶1PLC链接

图2-22所示为1∶N PLC链接，可实现多台PLC之间的数据交换。这里主站为CP1H机。从站除CP1H机外，还有CJ1M机。

提示：CP1H在CPU模块上可配置两个串口，但仅能用其中任意一个串口做PLC Link。否则系统将出错。

3. NT链接

利用串口，可进行NT，即可编程终端，链接，以实现可编程终端对PLC的监控。图2-23所示即为该连接的示意。图2-23a为1∶1链接，即一台PT监控一台PLC；图2-23b为1∶N链接，即多台PT监控一台PLC。

4. 无协议通信

利用串口，可使用串口通信指令，如数据发送（TXD、TXDU）、数据接收（RXD、RX-

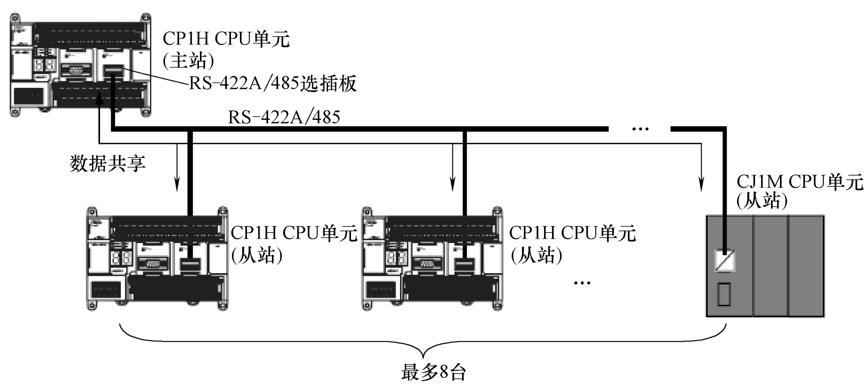


图 2-22　1∶N PLC 链接

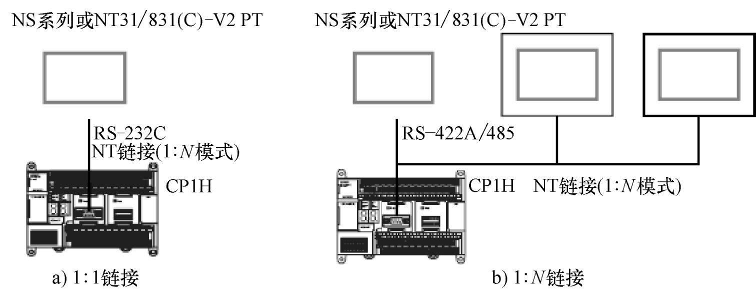


图 2-23　NT 链接

DU）等通信指令，实现与通信对象交换数据。有的 PLC 称这种通信为自由协议通信。

注意，这里虽无协议，但双方还是要有相关约定。通信时发送、接收数据的含义要按双方的约定处理。无协议通信用起来比较灵活，也比较方便。只是得编写、运行相应的 PLC 程序，否则什么通信也不会做的。

此功能可用于配置有 RS-232C、RS-422A、485 通信口的 PLC 与配置有相同串口的现场设备间的通信。也可用于主动与计算机通信。

5. 协议宏

协议宏是一组通信命令序列。可运用 OMRON 的协议宏编辑软件预先编辑。编辑好后，下载给通信单元，然后再运行宏指令（PMCR）予以调用。这样，调用一个宏命令，相当于运行多个的通信指令，以简化 PLC 的通信编程。

协议宏是 OMRON PLC 串口单元所特有的功能。如用于与 OMRON 的现场设备，如 OMRON 的温度控制器、智能信号处理器等通信，还有标准的宏序列。用户可直接调用。不然，用户也可按需要，自行编辑。图 2-24 所示为协议宏通信示意。

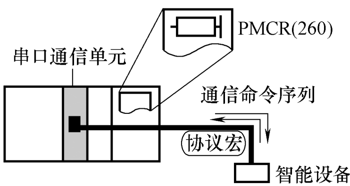


图 2-24　协议宏通信示意

6. 串口通信的其他功能

MODBUS-RTU 简易主站功能。这时设定串口为串行网关，发送 Modbus-RTU 命令。可用以控制变频器等 Modbus 对应的从设备。

2.3.3　OMRON PLC 串口设置

PLC 串口功能很多。到底要使用哪个功能，应在使用前做好相应设定。同时，还要设定有关通信参数，如波特率、奇偶校验、数据位等。设定可利用 CX-Programmer 编程软件的 PLC 设定窗口进行。图 2-25 所示为此设定窗口。

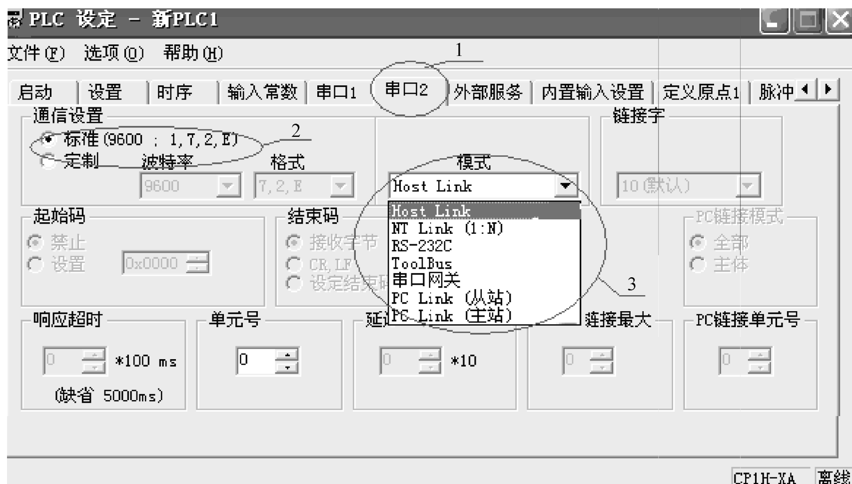


图 2-25　OMRON PLC 设定窗口

该图是对串口 2（见图中 1）进行设定。在图中 2 处，可设定通信参数。该图选标准，也可自己订制，由用户确定通信起始位、波特率、数据位及校验方式。在图中 3 处，可设定通信模式，实际就是确定串口的功能。该图选用 HostLink 功能，可用以与上位计算机通信。

如果选用 CP1H 机，除了 CPU 模块上配置两个串口，还可添加扩展 I/O 机架，再在机架上安装两个通信模块。每个通信模块都有两个通信口。因而，对 CP1H 机而言，最多可配置 6 个串口。

使用通信模块上的串口，也要利用 CX-Programmer 编程软件，对该模块进行设定。

如图 2-26 所示，它选用的 PLC（即新 PLC1）为 CP1H 机。设定时先在图 1 处（CX-Programmer 工程区的 IO 表和单元设置项）双击鼠标左键。之后，将弹出 PLC IO 表-新 PLC1 窗口。再在图 2 处（[0000] 主机架下 01 [000] 空槽）双击鼠标左键。之后，将弹出“选择单元”窗口。如选中该图 3 处的 CJW-SCU41-V1 通信适配器。单击该窗口的“确定”按钮，则弹出“添加单元”窗口。

此时，如在该窗口选择单元号为 1，单击“确定”按钮。图 2-26 的 2 处将变为图 2-27 的 2 处所示，即把 CJW-SCU41-V1 通信适配器添加到主机架上。

为了对这个适配器的功能及通信参数进行设定。还需在图 2-27 的 2 处双击鼠标左键，弹出 CJ1W-SCU41-V1 [编辑参数] 窗口，见图 2-27。这时，单击图中 1 处的“显示的参数组”项，如图 2-27 的 3 处所示，将显现该模块功能的设定菜单，可选择所要使用的功能。从图 2-27 可知，它的功能与 CPU 串口的功能基本上是相同的。除了选定功能，还可利用该窗口对该通信口的参数，如波特率等进行设定。

要说明的是，这里只讲对单元 1 上的 port1 进行设定。其实，对它的 port2 及单元 2 的串口也要进行设定。它的处理办法与上述是相同的。此外，所做的设定下载给 PLC 才能生效



图 2-26　通信适配器设定一

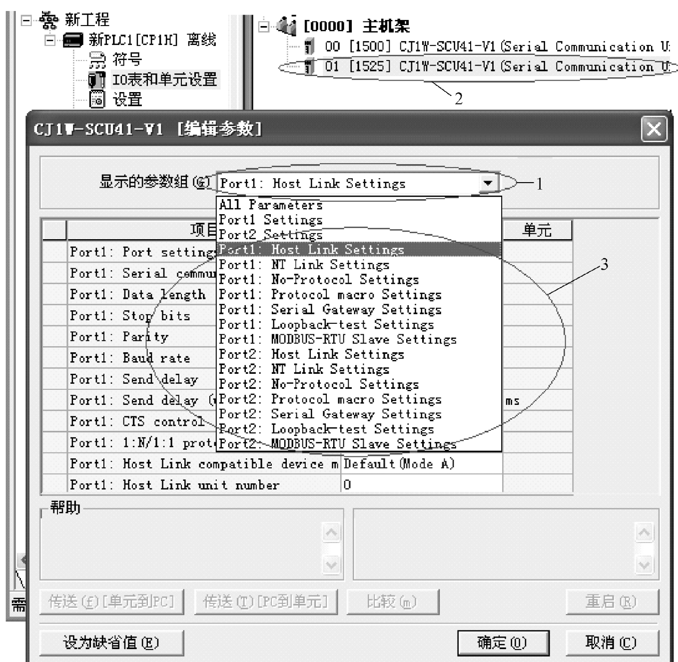


图 2-27　通信适配器设定二

（有的还要 PLC 重新上电后才能生效）。而下载之前，则须先把 PLC 置编程方式。

下载设定可以与程序下载一起进行，也可单独进行。还可在如图 2-28 所示的设置窗口的“选项”下单击“传送到 PLC”项实现。图 2-28a 所示为当计算机已与 PLC 联机，并已使 PLC 处于编程状态，单击菜单“选项”后所出现的下拉菜单。在其上 2 处就是“传送到 PLC”项，单击它即可向 PLC 传送所做好的设定。

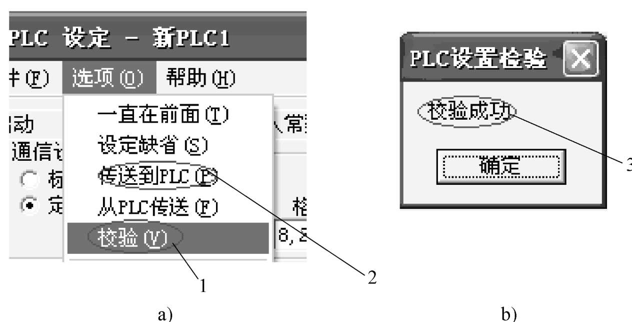


图 2-28　串口 1 设定下载

传送（即下载）后，可再在“选项”下拉菜单中，选图中 1 处的“校验”项，将进行是否下载成功的检查，如成功将弹出图 2-28b 所示的“PLC 设置检验”窗口，并提示“检验成功”（见图 3 处）。否则将显示“检验错误”。

提示：有时，设定下载后，须对 PLC 重新上电，设定才能生效，即检验才能成功。

除了使用编程软件设定，也可使用 CX-Net 网络配置工具设定。图 2-29 所示为 CX-Net 网络配置工具窗口。

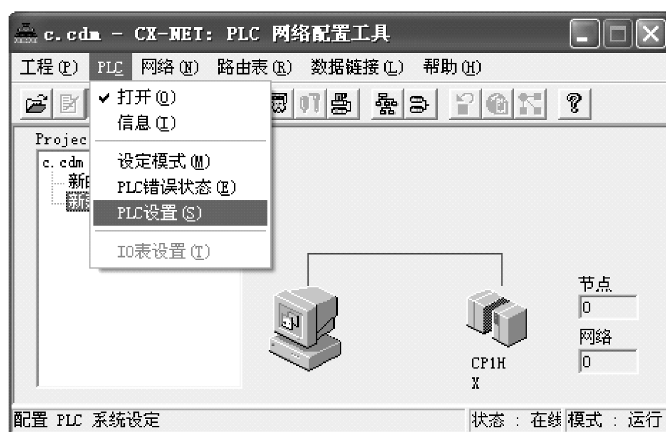


图 2-29　CX-Net 网络配置工具窗口

如图 2-29 所示，当所配置的计算机通过 USB 或串口与 PLC 联机打开后，单击“PLC”菜单项，将出现下拉菜单。再在其上单击“PLC 设置”，也可弹出如图 2-25 所示的 OMRON PLC 设定窗口。用它也一样进行相关设定。

在安装好 CX-Programmer 软件后，这个网络配置工具将自然生成，并在 Windows 的“开始”、“程序”、“OMRON”、“CX-One”、“CX-Programmer”项目下，单击“CX-Net 网络配置工具”项，即可弹出此窗口，如图 2-30 所示。

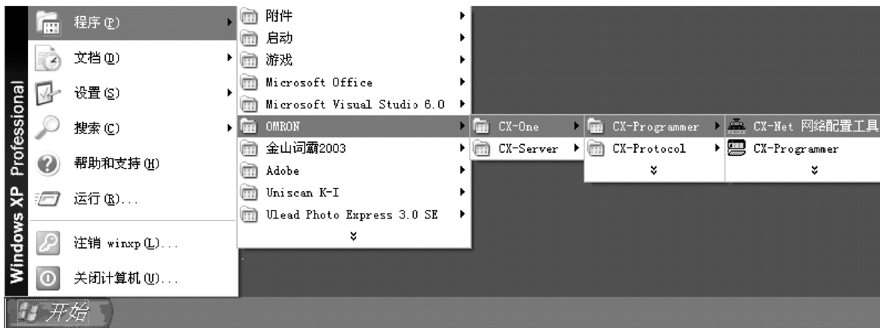


图 2-30　单击“CX-Net 网络配置工具”示意

2.3.4　OMRON PLC 串口连网实例

例 1　通过串口阅读条形码。

本例是在 CP1H CPU 单元上安装 RS-232C 选件板，并把它配置为无协议模式，用以阅读条形码，以识别不同货物编号。这在立体仓库的物件存储控制中很常用。图 2-31 所示为该配置简图。

这里，PLC 设定为 RS-232C 模式；程序仅使用接收数据指令。

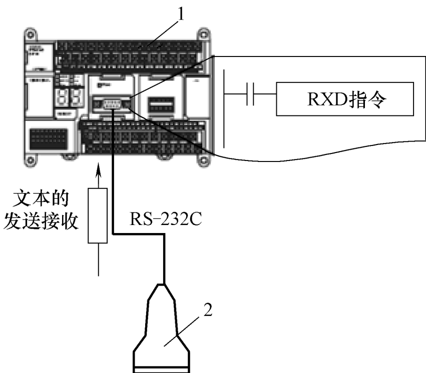


图 2-31　阅读条形码配置简图

例 2　Modbus-RTU 简易主站功能。

本例是在 CP1HCPU 单元上安装 RS-422A/485 选件板（或 RS-232C 选件板），并把它配置为串口网关模式，以作为 Modbus-RTU 主站。之后，对相应的 DM 区进行 Modbus-RTU 命令设定。这样，当 PLC 程序运行时，即可通过软件执行开关（操作相应的控制位 ON），而无须调用通信指令，即可向通信对方发送在 DM 区中设定的 Modbus-RTU 命令，以控制变频器等与 Modbus 协议对应的从设备。控制所接收的对方应答，也将自动保存到相应的 DM 区中。图 2-32 所示为该配置简图。

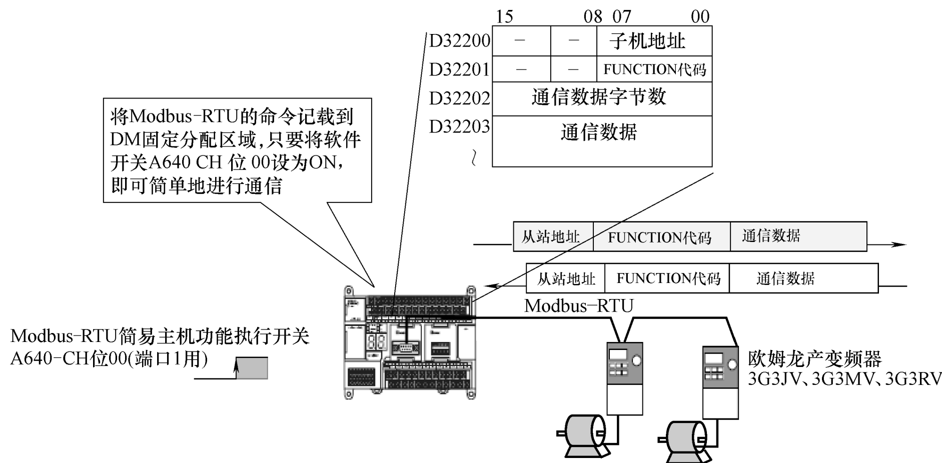


图 2-32　Modbus-RTU 主站配置简图

Modbus-RTU 命令设定使用的 DM 区与所使用的串口有关。串口 1 为 DM32200 ~ DM32249、串口 2 为 DM32300 ~ DM32349。保存 Modbus-RTU 回应信息的 DM 区也与串口有关。串口 1 为 DM32250 ~ DM32299、串口 2 为 DM32350 ~ DM32399。其中各字节的含义见表 2-9。而与所使用串口相关的辅助继电器，包括软件执行开关，见表 2-10。

表 2-9 Modbus-RTU 命令及应答用 DM 区的字及字节含义

通道		位	设定内容	
串行端口 1	串行端口 2			
D32200	D32300	07 ~ 00	指令	从站地址(00H ~ F7H)
		15 ~ 08		系统保留(请设为 00H)
D32201	D32301	07 ~ 00		FUNCTION 代码
		15 ~ 08		系统保留(请设为 00H)
D32202	D32302	15 ~ 00		通信数据字节数(0000H ~ 005EH)
D32203 ~ D32249	D32303 ~ D32349	15 ~ 00		通信数据(最大 94 字节)
D32250	D32350	07 ~ 00	响应	从站地址(01H ~ F7H)
		15 ~ 08		系统保留(请设为 00H)
D32251	D32351	07 ~ 00		FUNCTION 代码
		15 ~ 08		保留
D32252	D32352	07 ~ 00		出错代码
		15 ~ 08		系统保留(请设为 00H)
D32253	D32353	15 ~ 00		应答字节数(0000H ~ 03EA H)
D32254 ~ D32299	D32354 ~ D32399	15 ~ 00		应答(最大 92 字节)

表 2-10 Modbus-RTU 命令用辅助继电器

通道	位	对象串行接口	设定内容
A640CH	02	端口 1	Modbus-RTU 简易主站功能执行出错结束标志 1:执行异常 2:执行正常结束或执行中
	01		Modbus-RTU 简易主站功能执行正常结束标志 1:执行正常结束 2:执行异常结束或执行中
	00		Modbus-RTU 简易主站功能执行开关 0→1:执行开始 1:执行中 0:非执行中或执行结束
A641 CH	02	端口 2	Modbus-RTU 简易主站功能执行出错结束标志 1:执行异常结束 0:执行正常结束或执行中

（续）

通道	位	对象串行接口	设 定 内 容
A641 CH	01	端口 2	Modbus-RTU 简易主站功能执行正常结束标志 0→1：执行开始 1：执行正常结束 0：执行异常结束或执行中
A641 CH	00		Modbus-RTU 简易主站功能执行开关 0→1：执行开始 1：执行中 0：非执行中或执行结束

如果按通信对象命令要求，使「Modbus-RTU 简易主站功能执行开关」的操作（OFF→ON），所使用的 PLC 串口，将按照 DM 固定分配区域中设定的内容，把 Modbus-RTU 命令自动发出。其发送正常结或异常，都反映到相应的辅助继电器上。

例 3　PLC 链接配置一。

本例有 4 个 PLC 链接。主（母）站为 CP1H CPU 单元（或 CJ1MCPU 单元）。各从（子）站为 CP1H CPU 单元（或 CJ1MCPU 单元）。设定为全站链接方式。链接的通道（CH）数为 10CH。其配置及设定如图 2-33 所示。

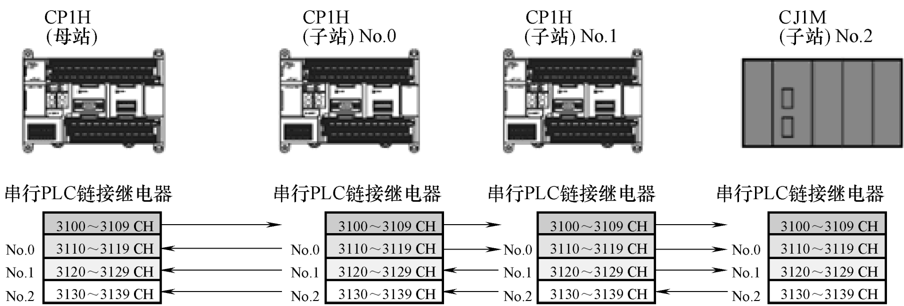


图 2-33　PLC 链接配置之一

其主站设定如图 2-34 所示。

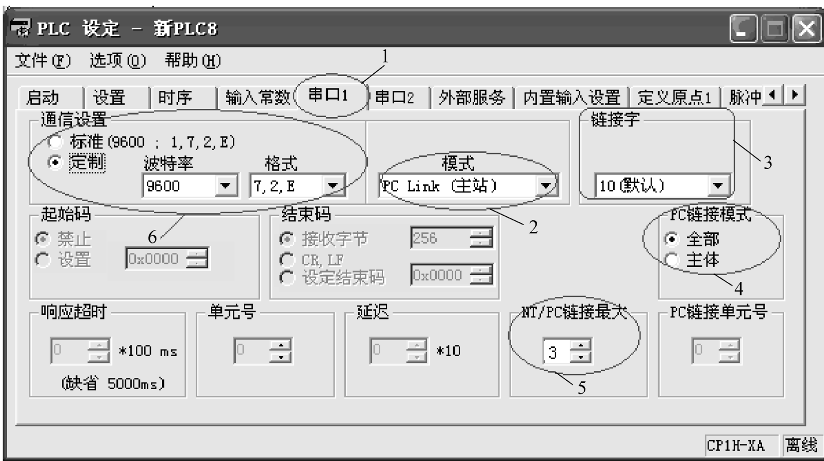


图 2-34　PLC 链接主站设定

从图知，它用的是串口 1（见图 1 处），设为主站（见图 2 处），通信设定为波特率 9600，格式为“7，2，E”（见图 6 处），链接字为 10CH（见图 3 处），链接方（模）式为“全部”（见图 4 处），链接 PLC 数为 3（见图 5 处）。

其从站 3 设定如图 2-35 所示。

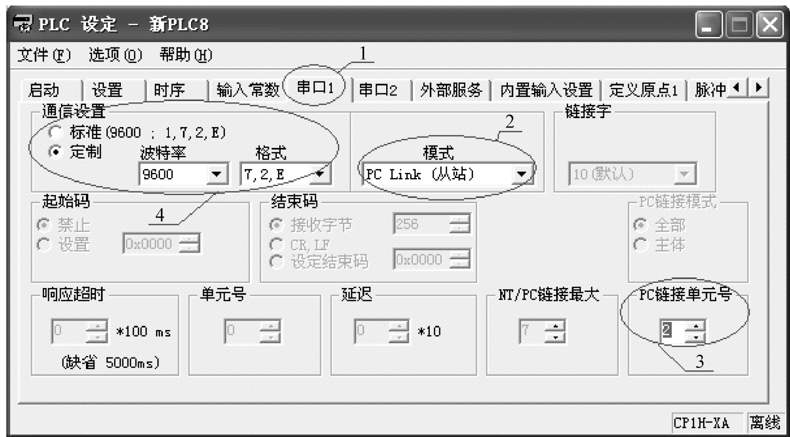


图 2-35　PLC 链接从站 3 设定

从图知，它用的也是串口 1（见图 1 处），设为从站（见图 2 处），通信设定与主站相同（见图 4 处），从占链接单元号为 2（见图 3 处）。其他从站也要作类似设定，具体略。

上述设定的含义是，所使用的链接地址为 3100～3139。其中主站的写区为 3100～3109，其余的为读区。No0 子站的写区为 3110～3119，其余的为读区。余类推。

把这些设定下载给各 PLC，当进行通信时，各 PLC 写区的内容将依次自动传送给各 PLC 相同地址的读区。这样，各 PLC 要向外传送的数据可写入自己的写区，而要使用别的 PLC 的数据可从别的 PLC 的写区读取，从而实现这几个 PLC 间的数据交换。

例 4　PLC 链接配置二。

本例有 4 个 PLC 链接。主（母）站为 CP1H CPU 单元（或 CJ1M CPU 单元）。各从（子）站为 CP1H CPU 单元（或 CJ1M CPU 单元）。设定为主站链接方式。链接的通道（CH）数为 10CH。其配置及设定如图 2-36 所示。

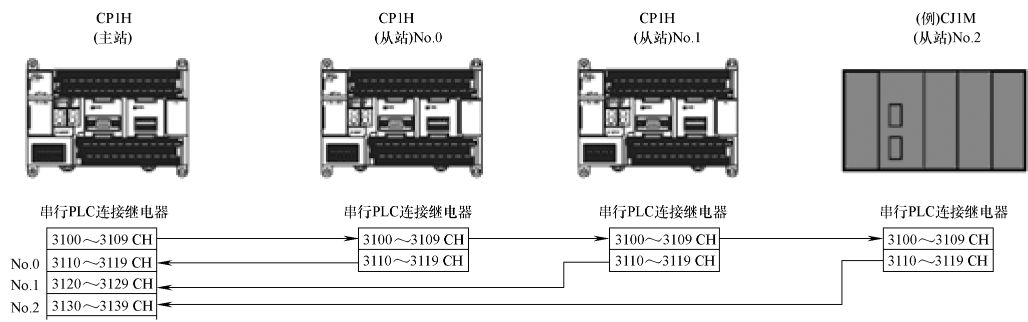


图 2-36　PLC 链接配置之二

其主站设定与图 2-34 不同的只是把链接模式改为“主体”。而从站设定不变。这样设定的含义是，主站所使用的链接地址为 3100～3139。其中主站的写区为 3100～3109，其余

的为读区。而各子站的写区均为3110~3119，而读区均为3100~3109。只是在主站上，对各子站的读区不同。对No0子站的读区为3110~3119，对No1子站的读区则为3200~3209、对No2子站的读区为3300~3309。

同理，把这些设定下载给各PLC，当进行通信时，主站PLC写区的内容将依次自动传送给各子站PLC相同地址的读区。而各子站PLC的写区，将分别写入主站的不同的读区中。这样，PLC主从站间即可很方便地实现数据交换。

这样设定的链接通信只是在主站与从站之间进行。从站之间不交换数据。但从站与通信相关的程序相同，便于程序共享。

例5 PLC串口通过移动网络与手机、计算机通信。

移动电话在我国发展很快。目前装机量已超过固定电话。所以，利用它进行PLC与计算机通信或与个人手机互发短信是很方便的。

为此，要有两台GSM的Modem，如BM2403A。还要有两张手机的SIM卡。系统配置如图2-37所示。

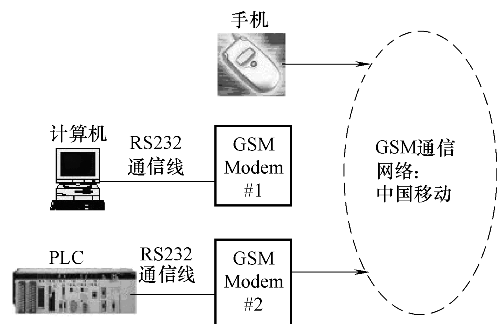


图2-37 PLC移动通信配置

此外，还要对串口特性、通信模式进行设置。把PLC串口要设置为无协议方式，特性与Modem一致。并编写调用TXD指令程序。

运行PLC程序后，当执行TXD指令条件具备，则自动发送AT指令给GSM Modem，Modem再将设定好的信息以短信的方式发送给用户手机、计算机。只要在中国移动通信的网络覆盖范围之内，就可收到此短信。

如发送“OK”。其AT命令为

AT+CMGS=“13912345678”（报头及手机号码）回车（结束符）OK（发送信息）发送符

以上为字符，实际要转换为ASCII码，并要预先存放在TXD指令的源字中。如它的开始字为DM100中，则对应的在DM100~DM112中的值（十六进制）分别为

DM100（4154，即字符AT），DM101（2B，即字符+C），DM102（4D47，即字符MG），DM103（533D，即字符S=），DM104（2231，即字符1），DM105（3339，即字符39），DM106（3132，即字符12），DM107（3334，即字符34），DM108（3536，即字符56），DM109（3738，即字符78），DM110（220D，即字符回车），DM111（4F4B，即字符OK），DM112（1A00，即字符! Nul）。

2.4 西门子PLC串口网络

关键词：PPI、MPI、自由协议、全局数据表、主站、从站

2.4.1 西门子PLC串口配置

1. S-200机串口配置

在S7-200 CPU模块上，集成有RS-485通信口。有一个口（Port0）的，有两个口

（Port0、Port1）的。两个口特性相同，但可各自属于不同的网络。可在不同模式、不同速率下工作，口地址也可相同。

利用这个串口，可与计算机连接通信。如计算机运行编程软件，则可实现计算机编程及监控，如上传、下载程序，监视数据变量，进行诊断。如计算机运行组态软件或用户应用软件，也可用以读取 PLC 数据，或向 PLC 下载数据。此外，还可与其他 PLC 或现场设备数据通信，进行数据交换。数据可以是数值数据，也可以是字符串。其他通信对象可以是：西门子变频器、其他上位机软件、第三方 PLC、第三方 HMI、第三方变频器、其他串行通信设备。

图 2-38 所示为 S-200 通信口。表 2-11 列出的为它的通信口引脚信号分配。

S7-200 CPU 上的通信口是非隔离型的，最高通信速率为 187.5K Baud/s。可并联连接多个端口。使用的连网介质为双绞线。

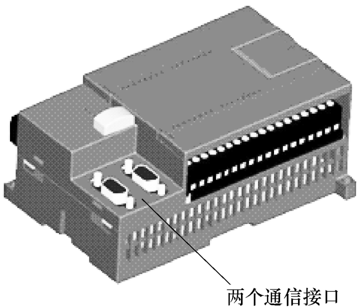


图 2-38　S-200 通信口

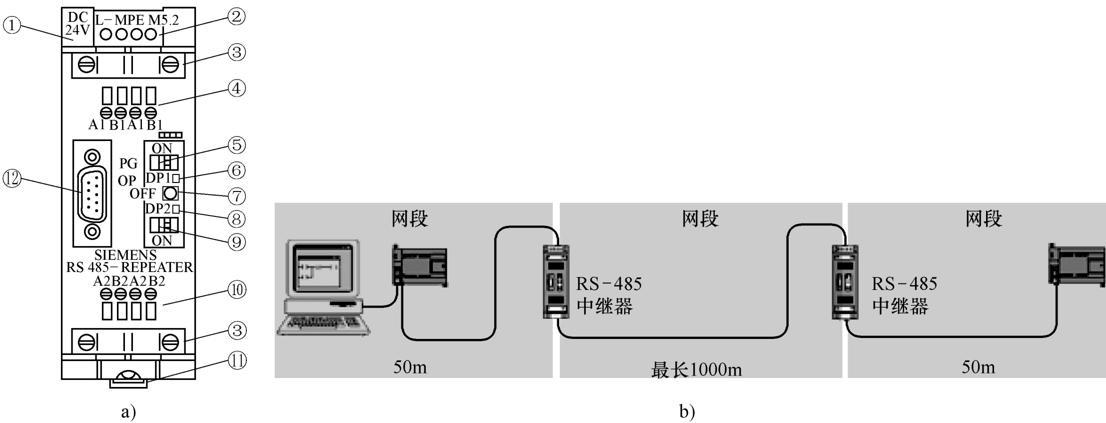
表 2-11　S7-200 通信口引脚信号分配

连　接　器	针　　号	信　　号	□0/□1
针1 针6 针5 针9	1	屏蔽	机壳地
	2	24V 返回	逻辑地
	3	RS-485 信号 B	RS-485 信号 B
	4	请求发送	RTS(TTL)
	5	5V 返回	逻辑地
	6	+5V	+V,100Ω 串联电阻
	7	+24V	+24V
	8	RS-485 信号 A	RS-485 信号 A
	9	未用	选择 10 位协议(输入)
	连接器外壳	屏蔽	机壳地

注：1. 3 和 8 为 RS-485 信号。通信端口可以从 2 和 7 向外供 24V 直流电源。
2. CPU 通信口上的 2、5 针在内部是连通的，并且它们和 CPU 上的直流电源（+24V）的 M 也是连通的
3. 通信口插座的金属壳、1 号针，与 CPU 接线端子上的电源部分的 PE 导通，而与上述的 M 不通拥有两个通信口的 CPU，其 Port0、Port1 的 2、5 针相通，也与 M 连通。

计算机通信口一般为 RS-232C。所以，不能与 S7-200 的串口简单相连。为此，西门子公司提供有专用电缆，即西门子提供有多主站 PC/PPI 电缆，可用于计算机的 RS-232C 口和 S7-200CPU 上的 RS-485 口连接。此外，西门子还提供有 USB/PPI 电缆，可用于计算机的 USB 口和 S7-200CPU 上的 RS-485 口连接。再就是西门子还提供计算机通信卡（称 CP 卡），也可用于 S7-200 编程。具体 CP 卡型号有，CP5611（用于 PCI 总线的 PC），CP5511/CP5512（用于笔记本电脑）。使用 CP 卡进行编程通信，应使用 MPI 电缆，或者 Profibus 电缆。

为了增大站点距离，可使用中继器，如图 2-39a 所示。站点间接入中继器的情况如图 2-39b 所示。



a)　　b)

①	RS-485 中继器电源的端子(如果要测量端子“A2”和端子“B2”之间的电压,则引脚“M5.2”为参考接地)
②	用于总线段 1 或 2 总线电缆的张力消除和接地的屏蔽夹
③	总线段 1 的总线电缆端子
④	总线段 1 的终端电阻
⑤	OFF 开关 (= 使总线段相互隔离,以进行诸如调试等)
⑥	总线段 2 的终端电阻
⑦	总线段 2 的总线电缆端子
⑧	用于安装和取下 DIN 轨上的 RS 485 中继器的滑块
⑨	总线段 1 上的 PG/OP 的接口
⑩	24V 电源电压 LED
⑪	总线段 1 的 LED
⑫	总线段 2 的 LED

图 2-39　中继器及其加接网络简图

在网络中，最多可以使用 9 个中继器，但是网络的总长度不能超过 9600m。还可为网络增加设备。如在 9600Baud/s 下，50m 距离之内，在一个网段，最多可以连接 32 个设备。而使用一个中继器允许在网络上再增加 32 个设备。同时，还可实现不同网段的电气隔离：如果不同的网段具有不同的地电位，将它们隔离会提高网络的通信质量。

在网络中，一个中继器也算做一个站点，但不必指定站地址。

此外，S7-200 机还可通过其 RS-485 口，接入 MPI 网。MPI（Multipoint Interface）是 SIMATIC S7-300、400 机的多点通信的接口，是一种适用于少数站点间通信的网络，多用于连接上位机和少量 PLC 之间近距离通信。但是，S7-200CPU 只能做 MPI 从站，即 S7-200CPU 之间不能通过 MPI 网络互相通信，只能通过 PPI 方式互相通信。而且 S7-300 或 S7-400 与 S7-200 通信时必须保证这个 S7-200 CPU 不能再作为 PPI 主站，Micro/WIN 也不能通过 MPI 协议访问作为 PPI 主站的 S7-200CPU。它的很多细节，可参阅有关说明。

此外，西门子 S7-200 机还有 EM241 模块，支持 V.34 标准（33.6K）的 10 位调制解调

器，用在模拟的音频电话系统（只支持模拟音频电话系统，不支持数字系统）中，可用以通过公共电话网，或小交换机系统进行远程通信。图 2-40 所示为 EM241 的外观图。

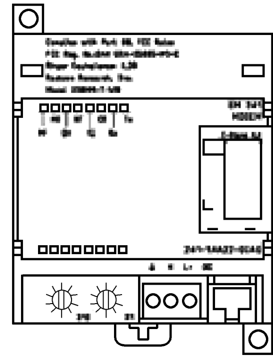


图 2-40　EM241 模块外观图

再就是，不使用 EM241，通过 RS-485 口也可直接连接 Modem。有线的、无线的均可。用它也可实现远距离通信。

2. S7-300、400 机串口配置

S7-300、400CPU 型号很多。各种 CPU 模块均集成有 MPI（多点接口），即 RS-485 串口。这既可做编程连接，又可组成 MPI 网。MPI 网可连接的设备有：PG（西门子编程器）/PC（计算机）、HMI（人机界面）、S7-300/S7-400，带有 MPI 的 S7-200（只适用于 19.2Kbit/s）。

对于所有 CPU 来说，一般（默认）传输速率为 187.5Kbit/s。如果与 S7-200 进行通信，也可指定 19.2Kbit/s 的传输速率。只有 CPU317 才能指定其他传输速率（最大 12Mbit/s）。

因为 MPI 接口为 RS-485，而计算机通信口一般为 RS-232C，所以不能直接接入。为此西门子公司提供有相关适配器（即转换电缆），PC-ADAPTER（适配器），用于 PC 的串口和 PLC 的 MPI 口直接连接。此外还有 CP5613、CP1613、CP5412A2 等通信卡。可支持 MPI、Profibus-DP 等多种协议，可用于工程师站/操作员站和 PLC 的多点连接。

MPI 的传输介质可以是屏蔽双绞线，也可以是光缆。使用双绞线其站点之间可串联最多 10 个中继器（见 S7-200 相关介绍）来加长连接距离，带中继器传输距离可达 1.1km。光缆带光连接器传输距离可达 100km。其拓扑结构可以是总线、星形、梯形分支连接，也可为环网。

MPI 通信电缆，LAN 连接器和 RS-485 中继器均采用 Profibus 和“分布式 I/O”系列产品。这些部件保证了最佳的配置。

MPI 网应用有成为提供多种服务的完整的网络；实施远程检测与诊断；远程编程；对等的全局数据交换；多个激活的在线连接。

对于和 PG/PC、HMI 系统以及其他的 SIMATICS7/C7/WinAC（西门子组态软件）自动化系统进行通信而言，MPI 是一种经济而又实惠的解决方案。最多可连接 125 个 MPI 站点，通信速率为 187.5Kbit/s。利用它可实现：

HMI 服务，由于其服务程序早已集成在 S7-300 的操作系统内，因此无需任何编程就能将数据传送到所连接的 SIMATIC 操作员面板或操作员站上。

MPI 还能作为一个 ProfibusDP 接口使用，允许配置 2 条 DP 线（只限于 CPU 318-2DP）。

MPI 网络还可实现全局数据（GD）服务。可周期性地相互进行数据交换。（每个程序周期最多允许 16 个 GD 包，每包最多 64 字节）。S7-300CPU 每次最多可以交换 4 个含 22 字节的数据包，而且最多可以有 16 个 CPU 参与数据交换（用 STEP7 V4.X 以上版编程软件）。

MPI 也可进行内部通信总线（K-总线）服务。其 PLC CPU 的 MPI 直接与 S7-300 的 K 总线连接，即可以用 K 总线接口从编程器直接通过 MPI 对 FM（西门子功能模块）/CP（西门子通信模块）模块进行编址。

除了 CPU 集成有串口，还有串口模块（通信处理器），CP340/341 及 CP440/441。可选用的串口有，RS232C（V.24）、20mA（TTY）（电流型串口，由主动方提供电流，只能连接

一个设备，最大距离 1000m，目前很少使用）及 RS422/RS485（X. 27）。使用它可实现点对点通信（PtP）。有的型号 CPU（例如 CPU314C-2PtP）也集成有 PtP 接口，以作为第二个集成通信接口。

点对点通信由于只有两个站点互连，用它替代总线系统，不仅功能非常强大，而且成本低廉，极为灵活、简单。可以选择不同的物理传输介质、传输速度，甚至可以选择自定义的传输协议。当只有少数（RS-485）设备与 SIMATICS7 连接时，点对点连接相对于总线系统的优势尤为突出。可进行这样点到点连接的设备有，SIMATIC S7 和 SIMATIC S5 可编程序控制器、打印机、机器人控制器、调制解调器、扫描仪及条形码阅读器等。

CP 340、341 特性及其比较见表 2-12。从表可知 CP 341 的功能、性能比 CP 340 要强些。

表 2-12　CP340、341 性能比较

		CP 340	CP 341
传输速率	最大值 最小值	19200bit/s 2400bit/s	76.8kbit/s 300bit/s
通信端口	RS-232C(V.24) 20mA(TTY) RS-422/485 (x.27)	y(340-1A) y(340-1B) y(340-1C)	y(341-1A) y(341-1B) y(341-1C)
传输协议	ASCII Printer-driver 3964(R) RK 512 customized	yes yes yes no no	yes no yes yes yes
最大传输距离	RS 232C(V.24) 20mA(TTY) RS 422/485 (x.27)	15m 1.000m 1.200m	15m 1.000m 1.200m
接口	串口	1	1

2.4.2　西门子串口通信协议

1. S7-200 串口协议

S7-200 串口支持的协议有：PPI 协议，MPI 协议，自由协议，USS 协议及 ModbusRTU 协议。

（1）PPI 协议

PPI 协议是西门子专为 S7-200 串口网络开发的主从协议。基于 Profibus 标准，并支持总线型与星形拓扑结构。可通过 RS-232 或 USB 接口进行数据传输。数据传输速率为 1.2kbit/s ~ 115.2kbit/s。其总线访问方法使用令牌传递规程。可以使用 RS-485 中继器扩展 PPI 网络。还可以将调制解调器连接至 PPI 网络。

PPI 是一种主-从协议：通信由主站发起，从站响应。主站可以与任何从站进行通信。从站只能根据主站要求做好应答。PPI 并不限制与任意一个从站通信的主站数量，但是在一个网络中，主站的个数不能超过 32。

主站设备为运行 STEP7 Micro/WIN 编程软件的计算机，或 HMI 设备（触摸面板、文本显示或操作员面板）。从站设备为 S7-200PLC。

如果使能 PPI 主站模式，S7-200 CPU 也可作为主站，可以使用网络读指令写指令来读写另外一个 S7-200。这也称为建立一个设备与设备之间的逻辑连接。这时，PPI 应设定为使用高级 PPI 协议。但是这个逻辑连接的个数是有限制的。S7-200 支持的连接个数见表 2-13。

表 2-13　S7-200 CPU 和 EM277 模块的连接个数

模　块		波 特 率	连 接 数
S7-200 CPU	通信口 0	9.6k、19.2k 或 187.5k	4
	通信口 1	9.6k、19.2k 或 187.5k	4
EM277		9.6k ~ 12M	6(每个模块)

当 S7-200 作 PPI 主站时，它仍然可以作为从站响应其他主站的请求。

PPI 协议是西门子内部协议，没有公开。但部分内容已被破解。此外，西门子还提供 OPC（PC Access）服务软件。计算机运行它的服务程序，可直接与 PLC 通信。用户的应用程序可调拥有关控件与此服务程序交换数据。这也可间接实现与 PLC 通信。

（2）自由协议

是建立在 RS-485 半双工硬件基础上的串行通信功能，其字节传输格式可以设置。一般为：一个起始位、7 位或 8 位数据、一个可选的奇偶校验位、一个停止位。凡是支持这个格式的通信对象，一般都可以与 S7-200 通信。使用自由协议，通信双方的约定完全由通信对象，或者用户确定。

使用自由协议，还可利用相关的指令库，按指令库定义的协议通信。如 USS 指令库定义的为 USS（Universal Serial Interface，通用串行通信接口）协议；再如 ModbusRTU 指令库定义的为 Modbus 协议。使用这些指令库的方法是使用前先添加指令库，然后再调用，等等。

这里的 USS 协议是西门子专为驱动装置开发的通信协议。其基本特点为：支持多点通信（因而可以应用在 RS-485 等网络上）；采用单主站的“主—从”访问机制；一个网络上最多可以有 32 个站点（最多 31 个从站）；简单可靠的报文格式，使数据传输灵活高效；容易实现，成本较低。这个协议可用于 S7-200 与西门子变频器（MM4 系列、SINAMICSG110 和老的 MM3 系列）通信。而这里的 ModbusRTU 协议通信，则是 Modbus 公司开发的，用于 PLC 与执行此协议的外设通信。

2. S2-300/400 串口协议

（1）MPI 协议

MPI 协议是西门子专为 S7-300、400 串口网络开发的。此网络站点除了计算机、西门子编程器，PLC 主要是 S7-300、400。如果要与 S2-200 PLC 通信，也可使用这个协议。但这时 S2-200 只能作为从站。

MPI 协议也是西门子内部协议，也没有公开。但西门子还提供通信服务软件 Prodave。计算机运行这个服务软件，可生成 Windows Api 函数。用户的应用程序可调这个函数，即可与 PLC 通信。

（2）其他协议

西门子 S7-300/400 的 PtP 接口或模块还有多种可供选用的通信协议，如 RK512、3964（R）以及 ASCII 及用户指定的协议（可重新装载）等。

3964（R）涵盖物理层与链路层。主要用在西门子 S5 系列机或第三方部件上，现在很少使用。

ASCII 协议（采用起始和结束字符或带校验字符）为简单的，用以连接到外部系统的协议。还可通过用户程序查询和控制接口的握手信号。

RK 512 涵盖物理层、链路层与传输层。3964（R）用于连接计算机。

用户协议可按需要使用。要使用哪个，就安装哪个协议驱动及使用哪个专项驱动特性。如 CP341，可装载的通信驱动软件，Modbus 协议 RTU 格式（主站）或 Modbus 协议 RTU 格式（从站），也可执行 AllenBradley DF1（美国 ABPLC 公司串口通信）协议。

提示：提供完备的各种连网组件是西门子 PLC 网络的一大特点。这也是别的 PLC 网络所没有的。

2.4.3　西门子 PLC 串口网络设定

在串口网络使用之前，必须对网络站点的地址、通信各方的串口，甚至使用的电缆都要进行设置，以确保各方通信参数相符。要记住西门子连网的格言：你糊弄它，它就糊弄你！设置的通信参数不相符，网络将无法顺利工作。

1. S2-700 机串口网络设定

（1）CPU 模块设定

新出厂的 S2-700 CPU 通信口的通信参数都有缺省设置，其通信速率为 9.6kbaud/s，站址设为 2。如要更改这个缺省设置，可在 Micro/WIN 软件或 Windows 的控制面板中打开 Set-PG/PCInterface 进行。事实上，对多站点的网络，这个更改则总是需要的。因为在同一个网络中，各个站的地址总不能都设为 2 吧！

为此，要更改通信口的地址。当然通信速率也可更改。这个更改可先在 S7-200 编程软件的 Communications（通信）窗口中进行。图 2-41 所示的即为该窗口，可用鼠标点击指令树中 Communications 项，或 View 菜单中的 Communications 图标打开。

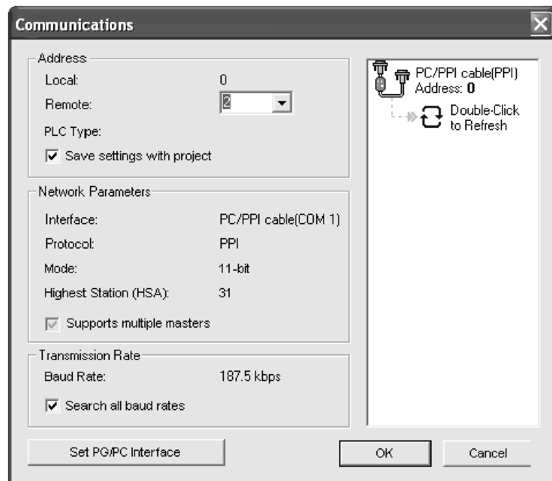


图 2-41　Communications（通信）窗口

在该窗口上，Local（本地）显示的是运行 Micro/WIN 的编程器（计算机）的网络地址。默认的地址为 0。使用 Remote（远程）下拉选择框可以选取试图连通的 S7-200 CPU 地址。缺省的地址为 2。可输入新值，予以更改。

这个更改也可先在 S7-200 编程软件的 Communication Ports（通信端口）选项卡中进行。图 2-42 所示为 Communication Ports（通信端口）选项卡窗口。

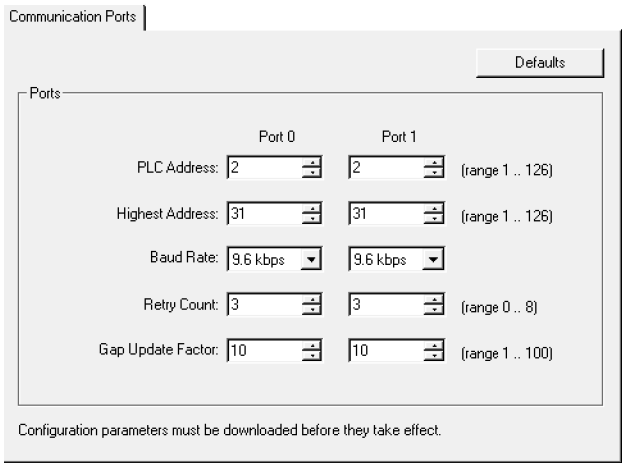


图 2-42　Communication Ports（通信端口）选项卡窗口

在该窗口中有：

PLC 地址（PLC Address）：设定 S7-200 CPU 通信口的地址。如果有两个通信口，它们的地址可以相同，因为两者不属于一个网络；

最高地址（Highest Address，HSA）：它定义一个主站寻找其他主站的最高地址。设置 HSA 限制了最后一个主站（最高地址）必须检查的地址间隙。限制地址间隙的长度可以最小化寻找和连接另一个主站所需要的时间。最高站地址对于从站地址没有影响。主站仍然可以与地址大于 HSA 的从站通信。总的规则是应该在所有的主站上设置相同的最高站地址。HSA 的缺省值是 31。输入通信网络上站点的最高地址；

波特率（Baud Rate）：设置通信速率。可从下拉列表中可以选择 9.6K、19.2K、187.5K；

重试次数（Retry Time）：输入通信失败时重新尝试的次数；

地址间隙刷新因数（GapUpdate Factor）：设置本站每隔几次获得网络令牌后，尝试在本站地址和下一个已知（活动）的主站地址的空间内寻找新加入的主站（仅在本站做主站时有效）。一般情况下使用缺省值 10 就比较合适。

该窗口左边括号中的数值是相应项可能的取值范围。

设置合适的最高地址和地址间隙刷新因数可以提高网络的运行性能。

假设一个网络中有 2 号站和 10 号站作为主站，（10 号站的）最高地址设置为 15。则对于 2 号站来说，所谓地址间隙就是 3 ~ 9 的范围；对于 10 号站来说，地址间隙就是 11 到最高站址 15 的范围，同时还包括 0 号和 1 号站。

网络通信中的主站之间会传递令牌，分时单独控制整个网络上的通信活动。网络上的所有主站不会同时加入到令牌传递环内，因此必须由某个持有令牌的主站定时查看比自己高的站址是否有新的主站加入。刷新因数指的就是在第几次获得令牌后检查一次高站址。

如果为 2 号站设置了地址间隙因数 3，则在 2 号站第三次拿到令牌时会检查地址间隙中的一个地址，看是否有新的主站加入。

设置比较大的因数会提高网络的性能（因为无谓的站址检查少了），但会影响新的主站加入的速度。

以上设置仅对通信主站有效。而 S7-200 是否也作为主站应在它的特殊寄存器 SM30、SM130 中设定（见关于自由协议通信设定）。对于 Micro/WIN、一些 HMI（人机界面）TD200 也有类似的设置。上述更改，即更改后系统块，要下载到 S2-200 的 CPU 中。下载后，新的设置才起作用。

（2）计算机与 PPI 电缆设置

首先，打开编程软件 Step7 Micro/WIN，如图 2-43 所示。在这个图的 View 上，用鼠标左键双击图标 Set PG/PC Interface（图的 1 处）（安装好编程软件 Step7Micro/WIN，在 Window 的控制面板上，也有此图标，双击它的效果相同），弹出 Set PG/PC Interface 窗口。

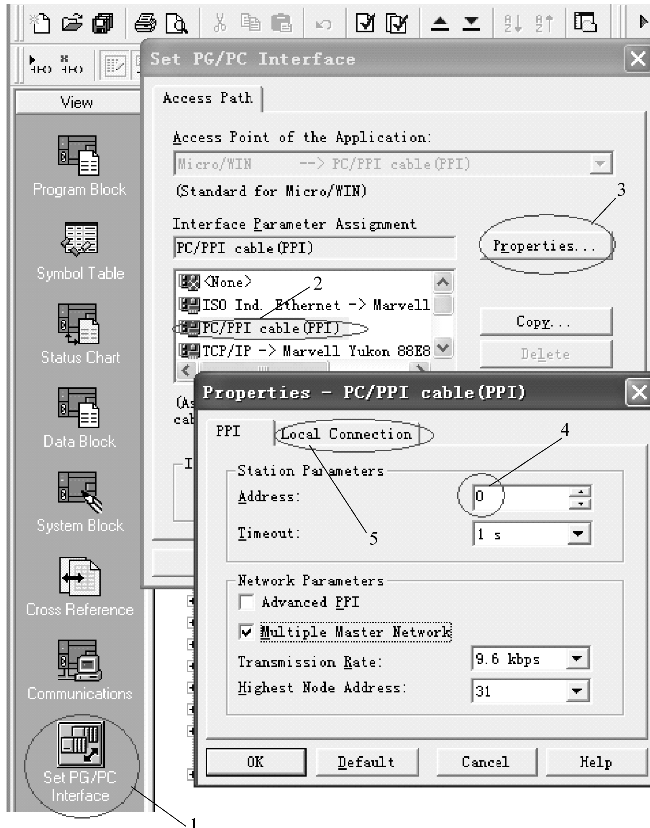


图 2-43　计算机方设置 1

接着，在 SetPG/PCInterface 窗口的 PPI 选择卡的 Interface Parameter Assignment（图的 2）处，选择 PC/PPI Cable（PPI）。

继而，点击 Properties 按钮（图的 3 处），将弹出 Properties-C/PPI Cable（PPI）窗口。可在其中的 Station Parameters 下的 Address 项（图的 4 处）选择本计算机的站点地址编号。本例地址选为 0。该窗口还有其他选项，也可作相应选择。

最后，选择使用计算机的那个串口或 USB 口。

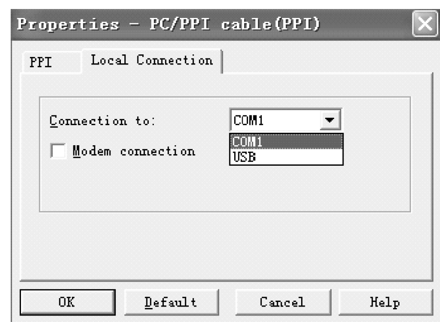


图 2-44　计算机方设置 2

办法是击 Local Connection 按钮，之后将出现 Local Connection 卡板，如图 2-44 所示，从中可对其进行选择。

至于电缆，如果使用的是智能多主站电缆（Micro/WIN V3.2 SP4 以上版），只需将 RS-232C/PPI 电缆的 DIP 开关 5 设置为“1”，而其他设置为“0”；而 USB/PPI 电缆不需要设置。老版本的电缆需要按照电缆上的标记设置 DIP 开关。

2. S7-200 串口自由协议通信设置

S7-200 CPU 的通信口可以设置为自由协议模式。为此，可通过用户程序把设置值写入特殊寄存器 SM30（用于 Port0）及 SM130（用于 Port1），进而完成设定。SM30 与 SM130 字节各位的含义见表 2-14。

表 2-14　SM30 与 SM130 字节各位的含义

□0	□1	描　述
SMB30 的格式	SMB130 的格式	自由口模式控制字节 MSB 7 … LSB 0 p p d b b b m m
SM30.0、SM30.1	SM130.0、SM130.1	mm：协议选择　00 = 点到点接口协议（PPI/从站模式） 01 = 自由口协议 10 = PPI/主站模式 11 = 保留（缺省是 PPI/从站模式） 注意：当选择 mm = 10（PPI 主站），PLC 将成为网络的一个主站，可以执行 NETR 和 NETW 指令，在 PPI 模式下忽略 2～7 位
SM30.2、SM30.4	SM130.2、SM130.4	bbb：自由口波特率　000 = 38400 波特　100 = 2400 波特 001 = 19200 波特　101 = 1200 波特 010 = 9600 波特　110 = 115200 波特 011 = 4800 波特　111 = 57600 波特
SM30.5	SM130.5	d：每个字符的数据位　0 = 8 位/字符 1 = 7 位/字符
SM30.6、SM30.7	SM130.6、SM130.7	pp：校验选择　00 = 不校验　10 = 不校验 01 = 偶校验　11 = 奇校验

设置为自由协议模式后，通信口就不支持其他通信协议（比如 PPI），S7-200 的编程软件 Micro/WIN 也将不能与 PLC 通信。但自由协议只能在 PLC 处于运行状态才生效。故只要把 PLC 重置于编程模式仍可与编程软件通信。此外，通过程序用值“00”重写 SMB30.00 及 00 位，按此重复定义后，将不再执行自由协议，也可恢复与编程软件通信。

如果调试时需要在自由协议模式与 PPI 模式之间切换，可以使用 SM0.7 的状态决定通信口的模式；而 SM0.7 的状态反映的是 CPU 运行状态开关的位置（在 RUN 时 SM0.7 = “1”，在 STOP 时 SM0.7 =“0”）

自由协议通信的核心指令是发送（XMT）和接收（RCV）指令。在自由协议通信常用的中断有“接收指令结束中断”、“发送指令结束中断”，以及通信端口缓冲区接收中断。

3. S7-300/400 串口设定

这个设定也称网络组态。要使用西门子编程软件。要做两个组态：一是 MPI 网络及其 PLC 站点的组态；二是全局数据组态。

（1）MPI 网络及其 PLC 站点的组态

MPI 网络组态是确定站点数，设定站点地址及网络通信有关参数。PLC 站点组态是选用 CPU 型号、电源、机架及信号模块等有关模块，以按要求构成 PLC 控制系统。其具体步骤是：

1）生成网络及其站点。以 3 个 S7-300 站点为例。其过程为：首先，在 STEP7 中生成 MPI 网络项目；其次，在 MPI 网络项目中生成 SIMATIC 300（1）、SIMATIC 300（2）及 SIMATIC 300（3）站点；最后，对每个站点分别确定选用的 CPU、电源及其他模块，进行硬件配置。配置的结果如图 2-45 所示。

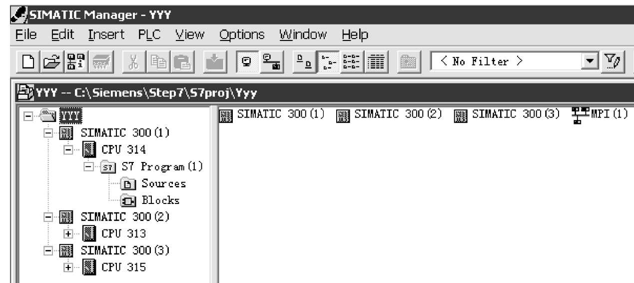


图 2-45　生成 MPI 网络及其站点

2）MPI 网络连接。在 MPI 网络项目中，双击“MPI 图标”，打开“NETPRO”窗口，选择 MPI（1）进行组态。这时，可对一条红线（MPI 网线）和三个互不相连的站点上建立连接。办法是分别用鼠标左键压住站的红点，并拖到 MPI 网线上。连接情况见图 2-46 MPI（1）网络连接。注意，连接完成后要存盘。

3）连接后再用鼠标右键点击各个站点，修改通信参数或进行各站点的硬件配置。具体过程与单机系统类似，这里不再赘述。

（2）全局数据表组态

如果要使用全局数据表链接通信，还需要进行全局数据表组态。其过程是：

1）生成空 GD 表。这可在图 2-46 所示的“NETPRO”窗口上，选中 MPI 网络线（变粗）。然后点击“OPTIONS”菜单项下的“DEFINE GLOBAL DATA（定义全局数据）”项。这时将弹出如图 2-47 所示空 GD 表。

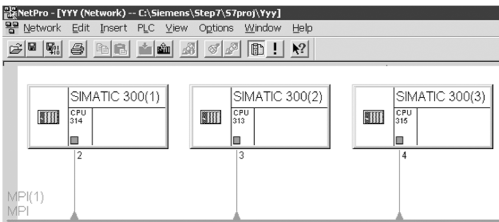


图 2-46　MPI（1）网络连接情况

图 2-47　空 GD 表

2）填写 CPU。双击“GDID”右边的方格，在出现的“SELECT CPU”对话框中双击站 1 的 CPU 图标，该 CPU 就出现在“GDID”右边的方格中。用同样方法将站 2 的 CPU 和站 3 的 CPU 放到对应的方格中。图 2-48 所示为已完成 3 个 CPU 的选用。

3）填写 GD 包。在 CPU 下面的一行中，生成 1 号 GD 环 1 号 GD 包中的 1 号数据。这可

GD - MPI(1)

GD Table Edit Insert PLC View Window Help

MPI(1) (Global data) -- YYY

	GD ID	SIMATIC 300(1)\ CPU 314	SIMATIC 300(2)\ CPU 313	SIMATIC 300(3)\ CPU 315
1				
2				

图 2-48 已完成 3 个 CPU 的选用

用鼠标右键点击 CPU 314 下面的方格，在出现的菜单中选择“SENDER”（发送者），该方格变深色，且在左端出现“>”符号。这时输入要发送的全局数据的地址 MW0。点击 CPU313 下面的方格单元，输入要接收的全局数据的地址 QW0。该方格的背景为白色，表示在该行中 CPU 313 是接收站。

用同样方法可以填写其余的 GD 数据。其示例如图 2-49 所示。

GD - MPI(1)

GD Table Edit Insert PLC View Window Help

MPI(1) (Global data) -- YYY

	GD ID	SIMATIC 300(1)\ CPU 314	SIMATIC 300(2)\ CPU 313	SIMATIC 300(3)\ CPU 315
1		>MW0	QW0	
2		QW0	>IW0	
3		>MB10:8	MB0:8	MB20:8
4		MB20:10		>DB2.DBB0:10
5		MB30:10		>QW0:5
6				

图 2-49 GD 数据包填写示例

提示：每行中应定义一个并且只能有一个 CPU 作为数据的发送方。要输入数据的实际地址。

这里变量引号“:”之后的数据为变量的复制因子，是用来定义数据区以字节为单位的长度。例如 MB20：8 表示数据区是从 MB20 开始的连续 8 个字节。而所占区域还要加上两个说明字节，共占 10 字节的区域。MW0:11 表示数据区是从 MW0 开始的连续 11 个字，加上两个说明字节，共占 24 个字的区域。

4）第一次编译 GD 表。其办法是，点击菜单项“GDTABLE”下的“COMPILE...”项。之后将生成 GD 环，如图 2-50 所示。例如，GD1.2.1 表示，1 号 GD 环 2 号 GD 包中第 1 组变量。

5）设置扫描速率。第一次编译 GD 以后，点击菜单项“VIEW”下的“SCAN RATES”项。之后，每个数据包将增加标有“SR”的行，如图 2-51 所示。这行可用来设置该数据包的扫描速率（1～255）。S7-300 默认值为 8，S7-400 默认值为 22。CPU-400 扫描速率设置为 0，表示是事件驱动的 GD 发送和接收。

6）设置 GD 包状态双字的地址。第一次编译 GD 以后，再点击菜单项“VIEW”下的“STATUS”项，将出现如图 2-52 所示的 GDS 行。可在其上给每个数据包指定一个用于反映状态双字的地址（不过此图中还没有给出此状态双字赋予地址）。其中 GST 是各 GDS 行中的状态双字相“与”的结果。有了这状态双字，可便于用户程序能及时了解通信的有效性和实时性，增强了系统的诊断能力。

GD - MPI(1)
GD Table　Edit　Insert　PLC　View　Window　Help
MPI(1) (Global data) -- YYY

	GD ID	SIMATIC 300(1)\ CPU 314	SIMATIC 300(2)\ CPU 313	SIMATIC 300(3)\ CPU 315
1	GD 1.1.1	>MW0	QW0	
2	GD 1.2.1	QW0	>IW0	
3	GD 2.1.1	>MB10:8	MB0:8	MB20:8
4	GD 3.1.1	MB20:10		>DB2.DBB0:10
5	GD 3.1.2	MB30:10		>QW0:5
6	GD			

图 2-50　第一次编译后生成的 GD 环

GD - MPI(1)
GD Table　Edit　Insert　PLC　View　Window　Help
MPI(1) (Global data) -- YYY

	GD ID	SIMATIC 300(1)\ CPU 314	SIMATIC 300(2)\ CPU 313	SIMATIC 300(3)\ CPU 315
1	SR 1.1	8	8	0
2	GD 1.1.1	>MW0	QW0	
3	SR 1.2	8	8	0
4	GD 1.2.1	QW0	>IW0	
5	SR 2.1	8	8	8
6	GD 2.1.1	>MB10:8	MB0:8	MB20:8
7	SR 3.1	8	0	8
8	GD 3.1.1	MB20:10		>DB2.DBB0:10
9	GD 3.1.2	MB30:10		>QW0:5
10	GD			

图 2-51　出现标有“SR”行的画面

GD - MPI(1)
GD Table　Edit　Insert　PLC　View　Window　Help
MPI(1) (Global data) -- YYY

	GD ID	SIMATIC 300(1)\ CPU 314	SIMATIC 300(2)\ CPU 313	SIMATIC 300(3)\ CPU 315
1	GST			
2	GDS 1.1			
3	SR 1.1	8	8	0
4	GD 1.1.1	>MW0	QW0	
5	GDS 1.2			
6	SR 1.2	8	8	0
7	GD 1.2.1	QW0	>IW0	
8	GDS 2.1			
9	SR 2.1	8	8	8
10	GD 2.1.1	>MB10:8	MB0:8	MB20:8
11	GDS 3.1			
12	SR 3.1	8	0	8
13	GD 3.1.1	MB20:10		>DB2.DBB0:10
14	GD 3.1.2	MB30:10		>QW0:5

图 2-52　出现标有 GDS 行的画面

7）以上设置下载个 PLC，然后运行 PLC，才能进行通信。

2.4.4　西门子 PLC 串口网络配置实例

1. 单主站 PPI 网络

其组成含有一个主站，一个或多个从站。STEP7-Micro/WIN 的编程设备/PC 或人机界面（HMI，例如：TD200、TP 或者 OP）作为主站。S7-200 作为从站。主站通过 PPI 多主站电缆或编程站上的通信处理（CP）卡与 S7-200CPU 发起通信。从站将响应来自主站的相关通信要求。

单主站 PPI 网络使用 PPI 协议。对图 2-53 所示的 Properties-C/PPI Cable（PPI）窗口配置时，不要选择多主站网络，也不要选中 PPI 高级选框。

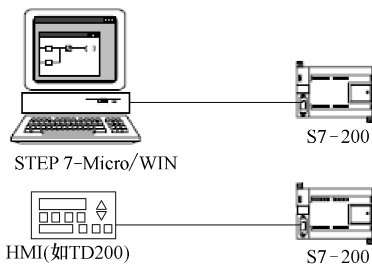


图 2-53　单主站 PPI 网络原理

2. 单主站多从站自由协议无线网络

计算机串口接无线 Modem，多个 S7-200 的各个 RS-485 串口也接无线 Modem，组成无线串口网络，使用自由协议通信。通信由计算机发起，PLC 响应。这个系统曾在威海市自来水公司使用，以远程管理 27 个供水系统的工作与采集有关数据。图 2-54 所示即为该系统配置简图。

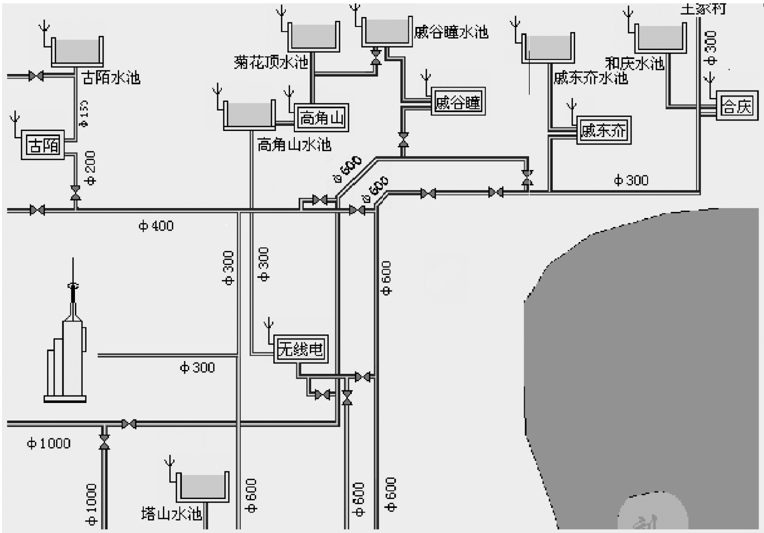


图 2-54　威海市自来水公司无线 Modem 网络简图

3. 多主站 PPI 网络

其组成含有多个主站，一个或多个从站，如图 2-55 所示。STEP7-Micro/WIN 的编程设备/PC 或人机界面（HMI，例如 TD200、TP 或者 OP）作为主站。S7-200 作为从站。每个主站均可通过 PPI 多主站电缆或编程站上的通信处理器（CP）卡与从站发起通信。从站将响应来自主站的相关通信要求。

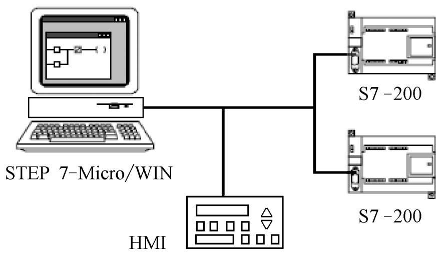


图 2-55　多个主站和多个从站

多个主站 PPI 网络，需使用 PPI 协议。对图 2-55 所示的 Properties-C/PPI Cable（PPI）窗口配置时，并应使能多主网络，并选中 PPI 高级选框。如果使用的电缆是 PPI 多主站电缆，那么多主网络和 PPI 高级选框便可以忽略。

4. 复杂 PPI 网络

图 2-56 示出的就是一个带点对点通信的多主网络的复杂 PPI 网络实例。除了计算机与 HMI 为主站，一个 S7-200 也设定为主站。每个主站可与从站发起通信。从站将响应来自主站的相关通信要求。同时，作为主站的 S7-200 可使用网络指令 NETR 和 NETW 指令读写从站 S7-200 PLC 的数据。

对于复杂的 PPI 网络，对图 2-56 所示的 Properties-C/PPI Cable（PPI）窗口配置时，最好使能多主站，并选中 PPI 高级选框。如果您使用的电缆是 PPI 多主站电缆，那么多主网络和高级选框便可以忽略。

5. 带有 S7-300、400 的 PPI 网络

图 2-57 所示的网络即为此实例。使用 STEP7 编程软件将 PPI 网络组态为 MPI 网络，并将 S7-200 作为从站设备。然后，S7-300、400 可以使用 X_PUT 和 X_GET 指令访问 S7-200 中的数据。网络波特率可以达到 187.5kbaud/s。但如果 S7-200 处于主站模式，那么 S7-300、400 将无法与之通信。

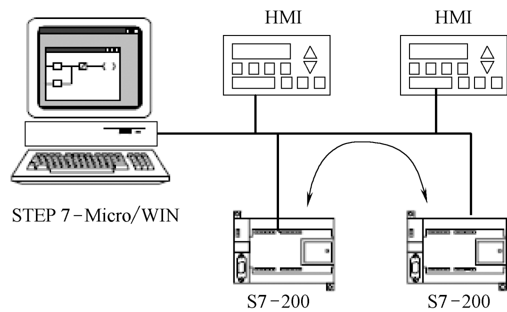


图2-56　复杂PPI网络原理

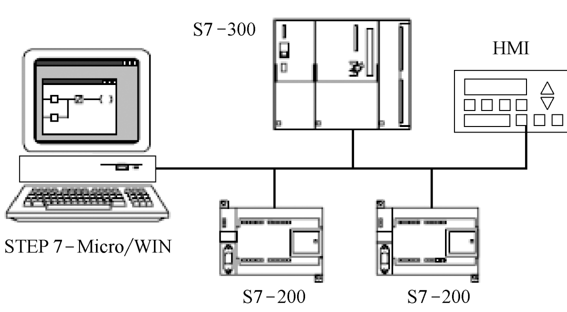


图2-57　带有S7-300、400的PPI网络

如果要求波特率高于187.5kbaud/s，那么S7-200 CPU必须使用EM277模块（Probufit模块）连接网络。同时，STEP7-Micro/WIN必须通过通信处理器（CP）卡与网络连接。

6. 计算机与S7-300相连的简单MPI网络

该网主要用来连接短距离的工程师站和操作员站，配置如图2-58所示。其组成为：一个工程师站/操作员站（ES，装有STEP7和WINCC软件）；一个编程适配器（将PLC的MPI口和ES的串口连接，以进行程序下载调试以及变量传输）；一个S7-300 CPU；一个电源模块（24VDC）和几个信号处理模块。

7. 计算机与S7-300相连的中等控制系统MPI网络

该网主要用来连接短距离的两个工程师站和操作员站，配置如图2-59所示。其组成为：一个工程师站/操作员站（ES，装有STEP7和WINCC软件）；一个操作员站（OS，装WINCC软件；两个5611/5613网卡（将PLC的MPI口和ES和OS连接，以进行程序下载调试以及变量传输）；一个S7-300 CPU；一个扩展机架；两个电源模块（DC24V）；几个信号处理模块。

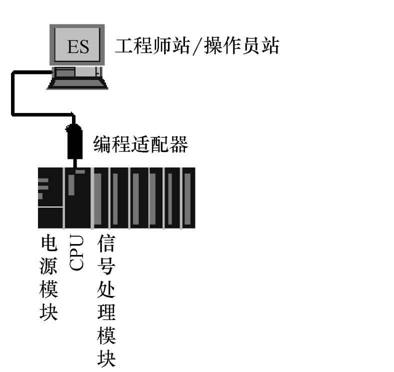


图2-58　计算机与S7-300相连的简单MPI网络

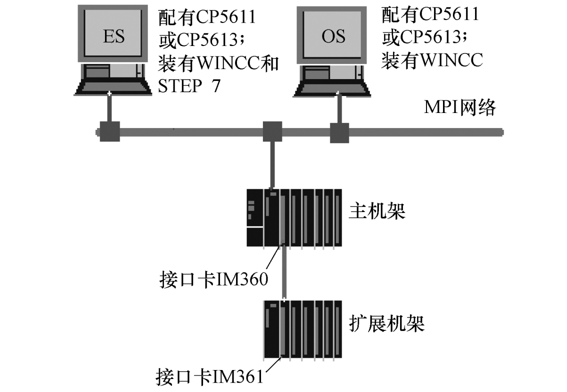


图2-59　计算机与S7-300相连的中等控制系统MPI网络

2.5　三菱PLC串口网络

关键词：内置串口插件板、串口通信模块、*N*∶*N*链接

2.5.1　三菱 PLC 串口配置

三菱目前主推的是 FX（小型）及 Q（中、大型机）PLC 都可配置多种串口。

1. FX 机串口配置

（1）所有 FX 机的主模块上都集成有 RS-432（编程）口

可使用三菱提供的电缆实现与三菱的简易编程器或计算机连接、通信。图 2-60 所示为该接口的外观及引脚的编号及功能。

（2）内置串口插件板

FX2N 还有串口选件，有 FX2N-232-BD、FX2N-385-BD、FX2N-422-BD。如 FX2N-232-BD，其安装过程示意如图 2-61 所示。

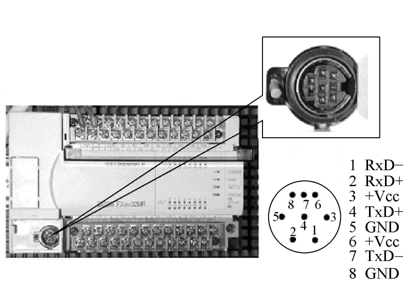


图 2-60　外设接口外观及引脚的编号及功能

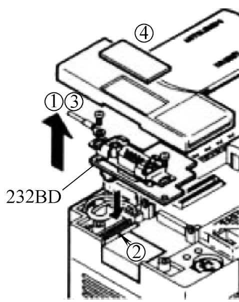


图 2-61　FX2N 串口选件安装过程示意

具体步骤为

① 从主单元的上表面卸下面板的盖子。

② 将 232BD 连接到基单元的板安装连接器。

③ 使用提供的 M3 自行攻丝螺钉将 232BD 固定到主单元上，将带有地线的圆插片端子和安装夹拧紧，保证插片型端子以右图所示方向固定，而且地线以下图中的方式从单元伸展出来。

④ 使用工具如钳子和剪刀，将面板盖子左边的孔剪掉，以便可看到端子块。连接器的上表面高于可编程控制器面板盖子的上表面，高大约 7mm（0.27″）。

其对应的端口定义，见表 2-15 所示。

表 2-15　FX2N-232-BD 端口定义

针脚号	信号	意义	功　能
1	CD(DCD)	载波检测	当检测到数据接收载波时，为 ON
2	RD(RXD)	接收数据	接收数据(RS232C 设备到 232BD)
3	SD(TXD)	发送数据	发送数据(232BD 到 RS232C 设备)
4	ER(DTR)	发送请求	数据发送到 RS232C 设备的信号请求准备
5	SG(GND)	信号地	信号地
6	DR(DSR)	发送使能	表示 RS232C 设备准备好接收
7,8,9	NC	不接	

内插板的优点是紧凑，不占额外空间。除了内插板，还有串口适配器，如 FX3u232ADP、FX3u485ADP、FX2NC232ADP 等，其功能与内插板相同。

（3）串口通信模块

如果以上串口还满足不了要求，还可另加多个串口通信模块，如 FX2N-232IF 的 RS-232C 通信特殊模块。

（4）FX3UC 串口配置

FX3UC 是三菱新型的 FX 机。串口配置功能更强。除了 FX 具有的配置，还可配置 USB 口（内置 FX3U-USB-BD）。它可用以实现与计算机通信。

2. Q 型机串口配置

三菱 Q 型机多都可作多种串口配置选择。

（1）CPU 模块上通信口

根据类型及型号的不同，都集成有不同的串口。如图 2-62 所示的 Q02H CPU 模块，既集成有 RS-232 串口，还集成有 USB 口。

（2）专用串口通信模块

如果 CPU 模块串口不足，还可配置串口模块。如图 2-63 所示为它的 3 种串口模块。其中 QJ71C24 可提供一个 RS-232、一个 RS-422/或 485，QJ71C24-R2 可提供两个 RS-232，QJ71C24-R4 可提供一个 RS-232 两个 RS-422/或 485。不过在实际配置时，所能增加的模块数量与选用的机型有关。

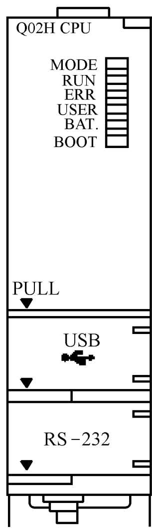


图 2-62　Q02H CPU 模块面板

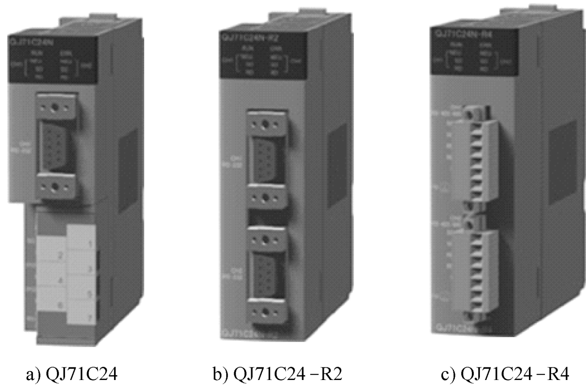


图 2-63　Q 型机串口模块

从图知，这里每个模块都有 2 个通信端口。这两个端口可同时使用，并可以设置不同的运行模式，以便用于各种不同的通信用途。

此外，还有调制解调器接口模块，即 QJ71CMO，是内置有用于连接公共电话线路的调制解调器的模块。可通过电话网络实现与远方计算机或其他设备通信。

2.5.2　三菱 PLC 串口功能

不管哪一种串口，大体都可实现如下功能：

1. 用于与计算机通信

可以 1（计算机）对 1（PLC），也可 1 对多 N 连接。有的还可 N 对 1、N 对 M 连接。连

接后可实现如下功能：

1）计算机运行编程软件（GX Developer）或网络管理软件，可实现对 PLC 的设定、编程、上载、下载程序；可对 PLC 的工作进行控制；可读取或改写，即收集和变更 PLC 数据。

2）计算机运行应用程序，可实现读取或改写 PLC 数据，对 PLC 控制系统实施监控。应用程序可使用协议编程。只是 FX 机与 Q 型机所用的协议不同。对 FX 机，有编程口协议与串口协议；对 Q 型机，有 MC（MELSEC 通信）协议。MC 协议还可用于三菱 PLC 的 Ethernet 模块通信。此外，也可使用三菱提供的通信软件，如 MX Component 等，不必弄清具体通信协议，也可编程。MX Component 与 MXsheet 软件配合，还可利用微软的 Excel 访问 PLC，读写 PLC 有关数据。

3）可编程控制器的通知功能，即 ON Demand 功能，也即 CPU 监视功能。可通过预先在 QJ71C24 中设置好监视条件，待该条件时间间隔和 CPU 内的数据状态成立时，QJ71C24 自动收集 CPU 内的数据，向外围设备发送。发生报警时也不用执行程序即可向外围设备传递报警信息，向对方设备发送必须通知对方设备的紧急数据。如果连接上调制解调器还可以通知传呼机。

2. 用于与其他 PLC 通信

1）链接功能。对 FX 机，可运用 $N:N$ 网络，或并联链接，通过设定或运行初始化程序，实现 PLC 间自动数据交换。

2）串口指令通信功能。一方或双方运行程序，执行 RS、RS2 等相关通信指令去实现通信。具体指令与机型及使用通信模块有关。这种通信也称无协议通信，即本书提到的自由协议通信。

3）Q 型机使用 QJ71C24 等串口模块，除了用 MC 协议与计算机通信，还可用无顺序协议、双向协议通信。其实，这里无顺序协议，也就是无协议，有的 PLC 称为自由协议。只是它执行串口模块用的通信指令。而双向协议执行的则是另一类串口通信指令。同时，双向协议通信执行接收指令，当接收完成后，会根据接收正确与否自动给对方发送相应的回应帧。执行发送指令，要受到对方发送相应的正确回应帧，才确定发送完成。所以，使用双向协议通信质量更有保证。

3. 用于与现场设备通信

可使用无协议实现可编程控制器与打印机、条形码读码器、检测仪器之类的外围设备通信，去采集和发送数据。通信协议由外围设备决定，而 PLC 方则配合外围设备的协议，运行相应的发送和接收通信指令组成的程序。

2.5.3　三菱 PLC 串口设定

使用串口前，要对串口的使用功能，工作参数进行设定。有两种设定方法：一为用编程软件设定；另一为用程序设定。

1. 软件设定

FX 机可使用 GX Developer 编程软件，也可使用早期的 FXGP-WIN-C 编程软件。Q 型机可使用 GX Developer 编程软件。

如果使用串口通信模块，还可使用专用软件 GX Configurator-SC。它作为插件安装在 GX Developer 中，可作为该模块的初始设定、监控/测试、编制数据通信处理所需程序时的支持

工具。要注意的是对串口模块设定时，首先要在 I/O 分配中将种类设定为“智能功能模块”。在实际的系统中进行 GX Configurator-SC 的设定时，请在可编程控制器 CPU 与串行通信模块已安装在基板上，与 GX Developer 连接的状态下进行。

2. 程序设定

就是运行 PLC 程序，对相关特殊继电器及特殊寄存器赋值，以达到通信模式、参数等设定的目的。三菱 PLC 的特点之一就是它的特殊继电器、寄存器特别多，各有几千个，而用于通信口设定的就不少。通信口用的这些特殊继电器、寄存器的功能与机型有关，从以下介绍的串口使用实例即可知晓。更详细的可参阅有关说明书。

2.5.4　三菱 PLC 串口使用实例

1. FX2N 机通过 RS-485 通信扩展板 *N*∶*N* 链接

其硬件配置如图 2-64 所示。

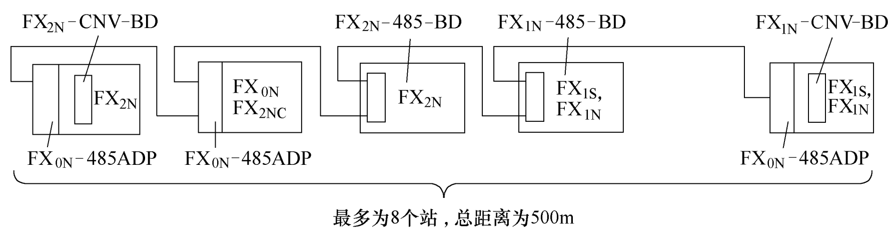


图 2-64　*N*∶*N* 链接通信硬件配置

具体接线如图 2-65 所示。

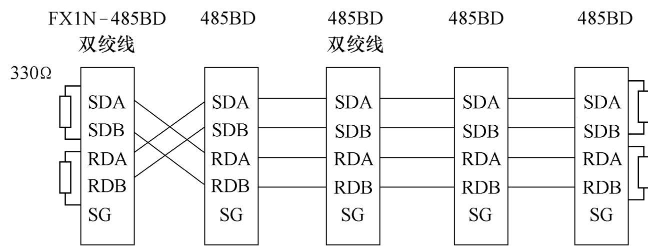


图 2-65　链接通信接线图

其网络设定：

主从站设定：在 D8176 中设。只能设定一个主站，其他为从站。指定为 0 的为主站，其他 1 ~ 7 为从站。注意，站地址不能重复。

从站数量设定：在主站 D8177 中设定。缺省为 7，即 7 个从站。在从站中不必设。

链接模式（规模）设定：在主站 D8178 中设。有 3 种可能设定，即 0、1 及 2。设为 0 时，4 字 D（D0 ~ D3，D10 ~ D13…余类推）参与链接；设为 1 时，除 D0 ~ D31，还增加 M1000 ~ M1031，M1064 ~ M1095…余类推；设为 2 时，规模比 1 增大一倍。即 D0 ~ D7，D10 ~ D17…余类推，及 M1000 ~ M1063，M1064 ~ M1127…余类推。详细见表 2-16。

重复次数：在主站 D8179 中设。

通信允许超时：在主站 D8180 中设，单位为 ms。

表 2-16 链接范围设定

站点号	模式 1		模式 2	
	位软件	字软件	位软件	字软件
	32 点	4 点	64 点	8 点
第 0 号	M1000 ~ M1031	D0 ~ D3	M1000 ~ M1063	D0 ~ D7
第 1 号	M1064 ~ M1095	D10 ~ D13	M1064 ~ M1127	D10 ~ D17
第 2 号	M1128 ~ M1159	D20 ~ D23	M1128 ~ M1191	D20 ~ D27
第 3 号	M1192 ~ M1223	D30 ~ D33	M1192 ~ M1255	D30 ~ D37
第 4 号	M1256 ~ M1287	D40 ~ D43	M1256 ~ M1319	D40 ~ D47
第 5 号	M1320 ~ M1351	D50 ~ D53	M1320 ~ M1383	D50 ~ D57
第 6 号	M1384 ~ M1415	D60 ~ D63	M1384 ~ M1447	D60 ~ D67
第 7 号	M1448 ~ M1479	D70 ~ D73	M1448 ~ M1511	D70 ~ D77

为了完成这个设定，必须运行初始化程序。图 2-66 所示为主站上使用的初始化程序。

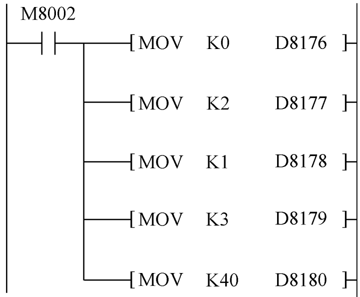


图 2-66 链接初始化程序

从图知，这里本站为主站，从站有 3 个，模式为 1，重复通信次数为 3，通信允许超时为 40ms。此外，还可利用通信过程的标志位，即有关特殊继电器的状态，检查是否出错。可根据出错情况作相应处理。这些标志位的含义见表 2-17。

表 2-17 通信出错标志及其含义

特　　性	专用继电器	名　　称	描　　述	响 应 类 型
只读	M8038	*N*:*N* 参数设置	选择 *N*:*N* 通信	主站、从站
只读	M8183	主站通信有错误	M8183 为 ON	主站
只读	M8184	从站 1 通信有错误	M8184 为 ON	主站、1 从站
只读	M8185	从站 2 通信有错误	M8185 为 ON	主站、2 从站
只读	…	…	…	…
只读	M8191	从站 8 通信有错误	M8191 为 ON	主站、8 从站

2. Q 型机使用串口模块实例

1）计算机通过它的 RS-232 口、RS-232 电缆及 PLC 的 QJ71C24-R2 模块与 PLC 相连，实现计算机与 PLC 通信，连线如图 2-67 所示。

2）计算机通过它的 RS-232 口、RS-232 电缆及 PLC 的 QJ71C24 模块与 PLC 相连，PLC 与 PLC 用 RS-485 电缆，实现计算机与 2 台 PLC 通信，连线如图 2-68 所示。

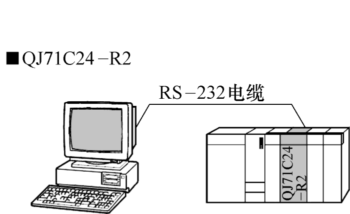


图 2-67　通过电缆、QJ71C24-R2 模块实现计算机与 PLC 相连

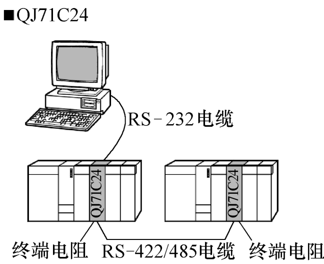


图 2-68　既与计算机相连又与 PLC 相连

3）计算机通过它的 RS-232 口、RS-232 电缆、调制解调器、公共电话线路及 PLC 的调制解调器接口模块 QJ71CMO 与 PLC 相连，实现计算机与 PLC 远程通信，连线如图 2-69 所示。如果系统要进行远程维护，这样配置是很常用的。

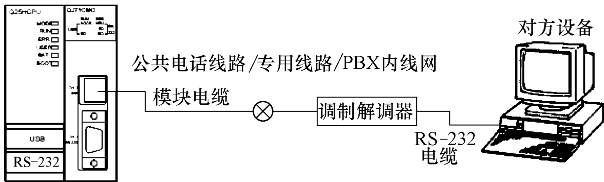


图 2-69　计算机与 PLC 远程相连

第 3 章　PLC 设备网及其配置

PLC 设备网是用以实现 PLC 与操作器、传感器等这样底层工业设备通信的网络。这些设备如限位开关、光电传感器、阀组、电动机起动器、过程传感器、条形码读取器、变频驱动器、物料流量计、电子秤、显示器和操作员接口等。有了这样网络，即使这些设备地处远程，PLC 也可向它或从它传送信号，实施对它的数据采集或控制。与处理地处当地设备不同的只是，处理时除了 I/O 刷新延时，还有通信延时。由于通信速率的不断提高，在绝大多数的情况下，这个通信延时都是允许的。而得到的好处则是，既可扩大 PLC 控制的范围、地域，又可节省昂贵和繁琐的硬接线。有的还可增加 PLC 控制 I/O 的点数。

本书第 2 章介绍的串口网络也可用于 PLC 与现场底层设备通信，但它通信速度低，通信站点少，与本章将介绍的设备网是无法比拟的。所以，大量现场设备要与 PLC 联网通信，还是要使用设备网。本章对 PLC 设备网的发展及其配置作简要介绍。

3.1　PLC 设备网概述

关键词：远程 I/O、总线、现场总线、现场总线标准

PLC 设备网是逐步发展的。最先是远程 I/O 网。它也是 PLC 最早的网络。20 世纪 80 ~ 90 年代，由于通信技术的进步，发展了现场总线技术。这对 PLC 设备网的影响很大。同时，由于 PLC 控制网及信息网的发展，也为 PLC 设备网的推进提供新的可能。设备网多为主从网，PLC 为主站，设备或设备连接的终端、从站模块及相关机架为从站。网络通信多是由主站发起，从站响应。

3.1.1　PLC 远程 I/O 网

早期 PLC 与远程工业设备通信用的都是远程 I/O 网。而且各个厂家的这个网络都不兼容。但共同的特点是，都有主站与从站模块。主站模块安装在当地 PLC 的机架上，受 CPU 管理，并通过机架上的并行总线与 CPU 通信。从站模块通过内部并行总线与安装在远程 PLC 的机架上的 I/O 模块通信，并管理这些 I/O 模块。而主、从模块间用的是串行通信，通过通信介质传递。可知，PLC 远程 I/O 网络实际是 PLC 部件间的通信。所以它的配置只是 PLC 的远程扩展配置。

这样配置不仅可以使 PLC 的 CPU 单元可以处理地处远程（如几百米或更长距离）设备的开关量（I/O）或模拟量（AD/DA）。同时，有时还可增加可处理的 I/O 总点数。

图 3-1 所示即为早期有名的 OMRON 公司的 C200H 机的远程扩展配置，也是 PLC 远程 I/O 网的一个实例。

从图知，它的远程主单元如同普通 I/O 单元一样安装于 CPU 机架（C200H 机可安装 2 个主单元）上。与这主单元相接的有两个从单元，分别安装在两个地处不同远处的从机架上。从图还知，该系统在当地仅一个机架 CPU 机架，而在第一远处有两个机架，在第二远

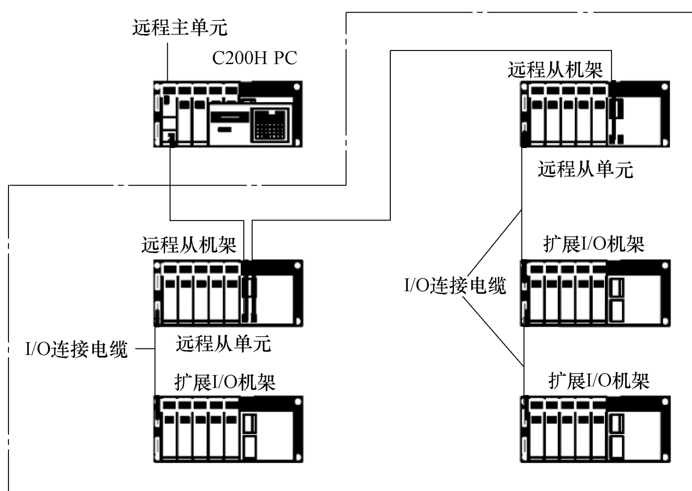


图 3-1　C200H 机远程配置

处有 3 个机架（这里讲的机架也就是母板，对 C200H 机这些母板是通用的）。C200H 机的远程配置的数据传输介质可以为双绞线，也可为光缆。只是其所使用的远程主、从模块有所不同。有了这样配置，远程设备可接入安装在远程机架上的 I/O 或 AD/DA 等模块，即可接受 CPU 的管理。与处理当地的设备相比，只是要增加通信所需的时间。

C200H 机做这样远程配置与仅为当地配置相比，还可使所控制的 I/O 点数增加一倍。

远程主单元除了连接远程从单元，还可连接远程终端。图 3-2 所示即为远程终端接口及其所连接的 I/O 模块。

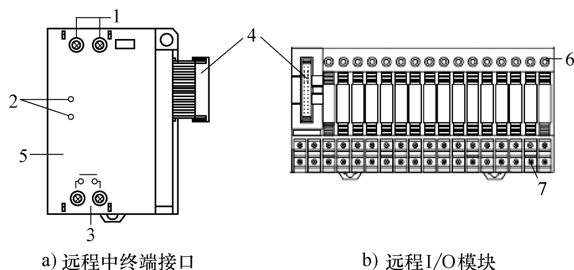


图 3-2　远程终端接口及其所连接的 I/O 模块

图中，1 为接口接线的端子，用于接通信双绞线。2 为指示灯，一为接电源指示，一为工作状态指示。3 为一对接点，当所接 PLC 处工作或监控方式，并传送无误时，ON，可用它实现监控。5 内为设定开关，其中 PIN6 无用，PIN1 ~5 为二进制编码设置终端号。4 为 I/O 模块连接器的插头与插座，可用它实现终端接口与 I/O 模块的连接。6 为 I/O 状态指示灯。7 为 I/O 接线端子。此外，I/O 板上还有输入电源端子，依型号不同可接直流或交流电源。

远程终端与远程机架的区别在于，它的点数少，更便于设备的多点分散控制。

除了远程机架及远程终端，若用的是远程光纤单元及光缆通信，还可通过 PLC I/O Link 单元，接 OMRON 小型 PLC。OMRON 也称这为 PLC I/O Link 网。一般讲，PLC I/O Link 单元有两个通道，一个为 I（输入），16 点。另一个为 O（输出），也是 16 点。同时，有两个身份。对所接小型机，它是其扩展单元；对远程主单元的 CPU，它是其远程终端模块。但两者的 I/O 的角色正好相反：如对所接小型机为 O，而对远程主单元的 CPU 则为 I，反之亦然。就是靠 PLC I/O Link 单元这个双重身份，加上在小型机及远程主单元的 CPU 上运行相应传送（MOV）指令，把要传送的数据发给各自的 O 区，并从各自 I 区读取数据，即可实

现小型机与远程主单元的 CPU 间的通信。有了这样的通信，远程主单元的 CPU 即可通过小型机实现对远程设备的控制。而这种控制可避免了远程 I/O 那样，数据采集、命令发送虽为远程，而控制仍是集中的。系统控制的风险可以减少。按照 PLC 网络各个站点能够独立工作（此工作本意应是能实施控制）的要求，才是真正意义的网络。

随着网络技术的发展，PLC 的远程 I/O 网也有了很大发展。主要有两点：一是把现场总线技术用于远程 I/O 系统；二是把原用于信息、控制网络这样的以太网及控制网的接口模块，也用作远程 I/O 模块。这既可提高 PLC 的远程 I/O 网络的通信速度及使站点的分布更加分散，又可使 PLC 控制网络化的组建更便捷、更经济、更好维护，进而也必将推进 PLC 控制的自动化系统的网络化和信息化。

3.1.2 现场总线

1. 现场总线概念

总线，英文叫“BUS”，原意为“公共汽车”。对计算机，是 CPU、内存、输入、输出设备传递数据的公用通道。对 PLC 网络或 DCS，它是各站点物理连接后传递数据的公用通道。前者传递数据多为同时传送多位数据，为并行总线，而后者传递数据为一位位数据顺序传送，为串行总线。

现场总线（Fieldbus）是用在现场的总线技术，把现场的操作器、仪表及其他设备与控制器进行物理连接、实施通信的串行总线。现场总线控制系统（Fieldbus Control System，FCS）是基于现场总线的分布式控制系统，是继 PLC、DCS（集散控制系统）之后出现的又一种新型的用于离散生产过程、连续生产过程及楼宇控制的自动化系统。根据国际电工委员会（IEC）标准和现场总线基金会（FF）的定义：现场总线是“安装在制造和过程区域的现场装置与控制室内的自动控制装置之间的数字式、串行、多点通信的数据总线”。现场总线把自动控制系统和设备带进了信息网络之中，形成企业信息网络的底层，从而为实现企业信息集成和企业综合自动化提供了更多可能。图 3-3 所示为传统的控制器与被控设备之间接线。

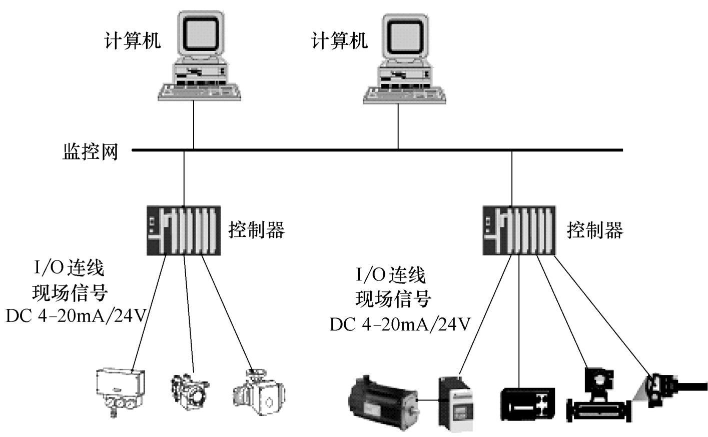


图 3-3 传统的控制器与被控设备之间接线

从图知，传统的控制系统其控制器与传感器或执行器之间的接线是并联的。如果传感器或执行器用的是开关量，则用连线传送 ON/OFF 信号；如果传感器或执行器用的是模拟量，

则连线传送（如 4～20mA 等），标准模拟信号。当控制器所控制的电器元件数量达到数十个甚至数百个时，整个系统的接线就显得十分复杂，容易搞错，施工和维护都十分不便。

图 3-4 所示为一种基于现场总线的控制系统结构简图。

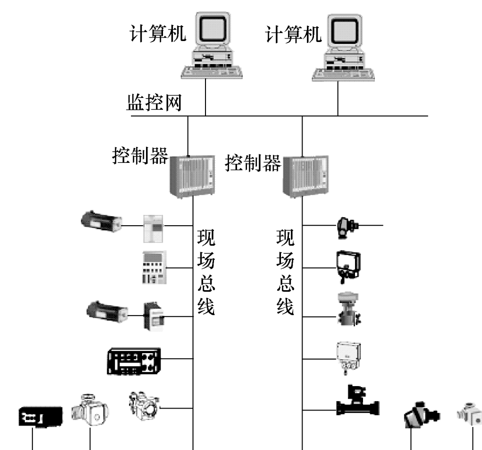


图 3-4　基于现场总线的控制系统结构简图

从图知，现场总线控制系统其控制器与传感器或执行器之间的接线是串联的。通过通信接口、通信介质实现它们之间的物理连接。同时，不管传感器或执行器用的是开关量，还是模拟量，都是用数字通信传送这些数据。这样，当控制器所控制的电器元件数量即使再多，整个系统的接线也比较简单，施工和维护也十分方便。

把图 3-4 与图 3-1 比较可知，现场总线与 PLC 远程 I/O 系统都是通过通信传送数据。但它们之间还是有很大区别的。相比之下现场总线具有以下一些特点：

（1）设备智能化

如果现场设备的接入是通过从站终端，那与当地的没有区别，不要求其智能化。而现场设备要单独接入，则要求设备要智能化。首先要有接入网络的接口；其次如果设备使用的是模拟量，还要能实现数模相互转换；再就是最好能进行信息处理以至于完成简单的回路控制。有了这样的现场设备才可将其单独接入网络，成为网络的一个站点。这样把一些简单的控制功能下放到现场，还可使控制系统具备高度的分散性，进而减低系统集中控制的风险。

（2）分布分散化

PLC 远程 I/O 系统的从站数有限，规模也较大，多与主站点类似，只是没有自身的 CPU。而现场总线从站数很多，规模多较小，甚至一个设备一个站点。完全可以是分散化的分布。正是这样的分布分散化，站点间又具有通信功能，更便于构成工厂底层控制网络。

（3）网络标准化

现场总线为开放式互连网络。其网络协议是公开的，有相应的国际或区域标准可依。只要按这些标准生产的产品就很容易接入该标准的网络，因而可接入的产品就会越来越多。这就给用户提供更多的选择不同品牌产品的机会，同时还不必为集成不同品牌产品而在硬件或软件上花费力气或增加额外投资。此外，由于使用的产品是按标准生产的，增加了互换性，为维修提供方便。

（4）效益最大化

由于有以上 3 个特点，引申之后就有这个效益最大化的特点。这里首先是，简化、节省与方便系统接线，降低系统的硬件成本。其次，可提高系统等可靠性，减少故障损失及系统维修费用。再就是，便于实现控制的网络化、信息化，从而带来附加效益。最后是系统便于重组，更能适应技术不断更新的要求。图 3-5 所示为使用 Profibus 现场总线系统与传统的系统对比的费用图表实例，说明使用现场总线可带来的效益。

2. 现场总线标准

现场总线的理念新、设想好，但要付诸实现，能够使相应地的工业设备能互连、互通及互操作，其前提是，要有被大家接受的标准。入网的产品都能按标准设计及制造。所以，制定现场总线标准是推进现场总线技术的关键。

由于商业利益的考虑，谁都想把自身已有的技术成为标准，所以，在形成这个标准中的竞争是很激烈的。以至于经过 10 多年的争论与妥协诞生了多个国际标准，具体是：

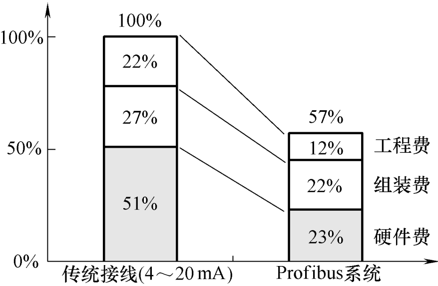


图 3-5 Profibus 现场总线系统与传统系统的费用对比实例

（1）IEC61158（IEC/TC65/SC65C）标准

它是国际电工委员会第 65 技术委员会下设的 SC65C 分会制定的。制订时间超过 12 年，先后经过 9 次投票，到了 1999 年，才制定出 IEC61158 标准第一版。后来又几经修改。最后，为了把已被工业自动化系统广泛采用的实时以太网（Real Time Ethernet，RTE）也纳入这个标准，诞生了 IEC61158Ed4 版本，有效期到 2012 年。该标准共推荐了经过市场考验的 20 种现场总线。表 3-1 示出了这 20 种总线。其中的实时以太网 EPA（Ethernet for Plant Automation）是我国提出的。

表 3-1 IEC61158Ed4 推荐的现场总线

类型	技术名称	类型	技术名称
Type1	TS61158 现场总线	Type11	TCnet 实时以太网
Type2	CIP 现场总线	Type12	EtherCAT 实时以太网
Type3	Profibus 现场总线	Type13	Ethernet Powerlink 实时以太网
Type4	P-NET 现场总线	Type14	EPA 实时以太网
Type5	FF HSE 高速以太网	Type15	Modbus-RTPS 实时以太网
Type6	SwiftNet 被撤消	Type16	SERCOS Ⅰ、Ⅱ 现场总线
Type7	WorldFIP 现场总线	Type17	VNET/IP 实时以太网
Type8	INTERBUS 现场总线	Type18	CC_Link 现场总线
Type9	FF H1 现场总线	Type19	SERCOS Ⅲ 实时以太网
Type10	PROFINET 实时以太网	Type20	HART 现场总线

（2）IEC62026（IEC/TC17/SC17B）标准

它是供低压开关设备与控制设备使用的控制器电气接口标准，于 2000 年 6 月通过。它包含以下几个总线标准：

1）IEC62026-1：一般要求；

2）IEC62026-2：执行器传感器接口 AS-i（Actuator Sensor Interface）；

3）IEC62026-3：设备网络 DN（DeviceNetwork）；

4）IEC62026-4：Lonworks（Local Operating Networks）总线的通信协议 LonTalk；

5）IEC62026-5：灵巧配电（智能分布式）系统 SDS（Smart Distributed System）；

6）IEC62026-6：串行多路控制总线 SMCB（Serial Multiplexed Control Bus）。

（3）CAN 总线标准

它是在 IEC61158 和 62026 之前，唯一被批准为国际标准的现场总线。CAN 由 ISO/TC22 技术委员会批准为国际标准 ISO11898（通信速率 < 1Mbit/s）和 ISO11519（通信速率≤125Kbit/s）。CAN 总线得到了计算机芯片商的广泛支持，它们纷纷推出直接带有 CAN 接口的微处理器（MCU）芯片。带有 CAN 的 MCU 芯片总量已经达到 1.3 亿片（不一定全部用于 CAN 总线），可见在接口芯片技术方面 CAN 已经遥遥领先于其他所有现场总线。

CAN 总线同时是 IEC62026-2 电器网络 DeviceNetwork（DN）和 IEC62026-5 灵巧配电系统 Smart distributed system（SDS）的物理层，它是 IEC62026 最主要的技术基础。

（4）所推荐的这些现场总线标准有如下特点

1）每一现场总线标准都有一到多家有实力的公司支持，并都有受这些公司支持的独立厂商组织，负责管理这个总线的规范及支持在全球范围发展的推广，都力求推进自身的系统。

2）每一现场总线标准都已在一定领域得到实际应用，已成为该领域的主导现场总线。

3）推荐的标准虽多，但其中也有交叉，即也有技术相互借用的部分。如 DeviceNet 用到了 CAN 的底层技术等。

4）国际标准推荐的总线虽多，但有的与 PLC 关系不大。与 PLC 有关的可用于实现 PLC 与现场设备通信，也可用于 PLC 之间通信，有的还可用于 PLC 与计算机通信。这意味着 PLC 的设备网、控制网及信息网都可用到现场总线技术。

5）计算机及 PLC 网络技术还在发展，所以，标准内容还在增加，争论也不可能停止。事实上，那么多标准推荐的那么多现场总线，也只是一时的妥协，或对各自应用领域的划分，远不是真正的国际统一的技术标准。

6）面对现场总线多标准的现实，不少厂家也改变了执行单一标准的策略，而是设计与制造可执行多个标准的不同产品，使自身的产品能与多种现场总线接轨，为自身产品开拓更大的应用空间。

3.1.3　PLC 设备网

经过多年发展，目前 PLC 的设备网有 3 类：一是 PLC 公司专用的，主要是 PLC 远程 I/O 网，只能接入本公司的产品或非智能的现场设备；二是基于现场总线标准的开放设备网，可与具有相应标准通信接口的设备或其他 PLC 连网；三是控制网或信息网扩展而成的远程 I/O 网络，通信速率很高，也有一定的网络标准可循，已出现相互兼容的可能。

由于 PLC 公司专用远程 I/O 网存在固有的不足，目前已逐步退出，只是老产品还在使用，所以，本书将不再对其进行介绍。至于控制网或信息网扩展而成的远程 I/O 网络，由于与控制网、信息网联系密切，本书将合并在介绍这两个网络的章节中一并说明。这样，本章以下各节将只分别介绍几种基于现场总线的设备网。具体是：AS-i、CompoNet 及 CC-Link/LT。先对这些网络作简要的综合说明，然后再介绍有关公司的这类产品及其应用实例。至于还有一些现场总线网络，如 DeviceNet、CC-Link 及 Profibus，也可用于组建设备网，但它们还可实现 PLC 之间的通信，为便于叙述，本书将它们放在 PLC 控制网一章一并介绍。

3.2 AS-i

关键词：AS-i、AS-i 主站、AS-i 从站、2.0 版本、2.1 版本、APM 信号、缓冲区、编址器、监控器

AS-i 首先由德国人于 1990 年提出并开始研发，1994 年开始加以推广与应用，并与当时欧洲几大行业公司联合成立了 AS-i 社团组织。后来逐渐发展壮大，吸纳了世界著名的传感器、执行器制造商和研究单位，发展成为国际 AS-i 组织。主要参加单位包括：P+F、FESTO、西门子、ASINTERNATIONAL、ITEI、SEARI、TSINGHUA 等。在 ASI 国际联合会的大力支持下，于 2003 年在北京成立了 ASI 中国协会，参加的有国外自动化领域的著名大公司，国内大学和研究机构，并将吸收国内企业加入。

AS-i 总线技术成熟，简单可靠，费用较低，应用广泛。不仅成为国际标准（IEC62026-2），并且也成为中国的国家标准（GB/T 18858.2—2002）。

3.2.1 AS-i 简介

AS-i 属于最底层设备级的总线，可用来在控制器（主站 Master）和传感器/执行器（从站 Slave）之间双向交换信息的主从网络。主要针对"位"一级数据传输的执行器、传感器使用。它处在控制网络的最底层，而对顶层是开放的。与其他现场总线不仅不存在竞争，而且还是其他现场总线在技术上和经济性上的补充。图 3-6 所示为 AS-i 与其他工业网络的关系简图。其中三角形标志为它的图标。

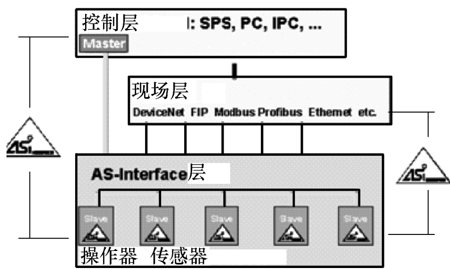


图 3-6 AS-i 与其他工业网络的关系

AS-i 有多个版本。其中 2.1 版本（AS-Interface Specification Version2.1）是 2002 年 AS-i 国际协会发布的，该版本在保证对旧版本技术标准完全兼容的前提下，对 AS-i 总线系统做了改进。最主要的改进有以下 3 个方面：总线上一个主站所能控制的最多从站数量由 31 个增加到 62 个；具有更加强大的错误诊断功能；具有更加简单、规范的模拟量的传送方式。

目前世界上主流的 AS-i 总线系统产品已经都是按照 AS-i 总线技术规范 2.1 版本生产的。表 3-2 列出了 AS-i 新旧版本技术规范中的不同功能之处。

表 3-2 AS-i 新旧版本技术规范比较

版本 / 功能	2.0 版本的技术规范	2.1 版本的技术规范
站点总数	31 个从站和 1 个主站	62 个从站和 1 个主站
输入/输出比特	4/4	4/3
模拟量传送能力	可以，但不是标准的，要加新模块并编写程序	可以，标准定义的，很方便
网络中总的输入/输出端口数	124 输入/124 输出	248 输入/186 输出
最大周期数	5ms	10ms
网络中最多可以传送的模拟量数目		124 路模拟量

1. AS-i 网络组成

AS-i 网络组成如图 3-7 所示，有主站、从站、电源及网络附件 4 个部分。

（1） AS-i 主站（MASTER）

AS-i 主站由配置有 AS-i 主站模块（AS-i 主机）的控制器（如 PC、PLC 等）或网关（用以连接 Profibus 或以太网）组成，在网络中必须有一个，也仅能有一个。网络通信由主站发起，从站相应。

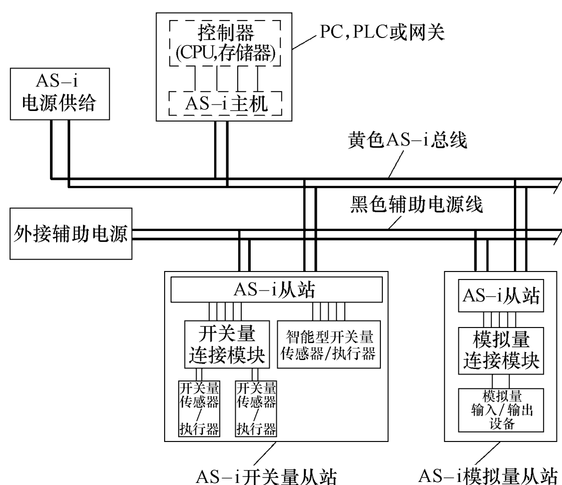


图 3-7　AS-i 网络组成

主站除了与从站轮循传送信号，正常读写从站数据之外，还具有以下功能：向每个从站传送参数配置，连续地进行网络运行监控，并进行故障诊断。

（2） AS-i 从站（SLAVE）

具体有：

1）I/O 从站终端（模块），可用于连接现场普通 I/O（开关量）。其防护等级有 IP20 及 IP65/67。前者用于在控制柜内安装；后者用于在恶劣现场直接安装。

2）智能型从站。这类传感器、操作器内置有小巧，但是功能强大 AS-i 从站芯片，有自己的从站地址。例如，智能按钮/指示灯，信号灯柱、传感器、电机起动器、隔膜键盘等。

3）逻辑模块。如西门子 LOGO 微型 PLC，如安装有 CMAS-I 模块（其上也配置有 AS-i 从站芯片），也可连接到 AS-i 网络上，作为 AS-i 站。连接后，每个 LOGO 可以在网络上有 4 输入/4 输出（共 8 个）开关量与主站数据交换。

（3） 供电单元

在 AS-i 系统中，电源是非常重要的模块，与一般电源有很大不同。它除了供电，将 AC 220V 转换为 DC 30V，还要进行平衡网络、数据解耦及安全隔离。

平衡网络是为了在对称的、非接地条件下工作能达到 EMC（防辐射）要求。为此，其屏蔽线要接地，在 AS-i 网络中也只允许该点接地。

数据解耦由两组并联的 39Ω 电阻和 50μH 电感组成，利用电感对电流的微分作用，把 AS-i 发送的电流信号转换成电压信号，并且可以在电源发生短路时对网络进行一定程度的保护。

（4） 网络部件

有电缆、中继器、分支器、扩展器等。

1）电缆。用于 AS-i 设备之间物理连接，既要传输信号，又要提供电源，在选择电缆时必须注意两个技术指标：一是通信频谱特性，二是直流阻抗特性。在有较大干扰的情况下，需使用屏蔽电缆，但它也必须满足规定的频谱特性要求。特别要注意的是屏蔽层在 AS-i 电源端只能接地，而不能接在 ASi + 和 ASi – 端。

AS-i 总线推荐使用的电缆有黄色和黑色扁平电缆。不同颜色的规范电缆都可使用独特的绝缘穿刺连接技术，可使系统连线完全不用剪断或拆除电缆或电缆芯的绝缘皮。而且只有在极性正确的情况下，电缆才能被放入设备中。现在这种黄色的电缆已经成为 AS-i 的一种商标，几乎成了 AS-i 的代名词。而黑色的电缆则用于输出模块和部分输入模块与辅助电源

连接。辅助电源加入不是必要的，要根据需要而定，目的是避免 AS-i 通信电压过低。

AS-i 规范电缆芯线绝缘材料通常是橡胶混合物（EPDM）。对于要求较高的应用场合，如要求防化学制剂腐蚀的场合，可以选用规范的 TPE（热塑性弹性体）和 PUR（聚氨酯）电缆。当然，也可以选用无 PE 导线的圆形双线电缆。

2）中继器、扩展器及分支器。如果系统的布局要求电缆的长度超过 100m 时，网络可以通过添加中继器扩展到 300m，每个中继器可以向外扩展 100m 的网段。从站可以连到任何 AS-i 的网段上，但每个网段要有自己的电源模块。由于中继器在两个网段之间可以实现电气隔离，这样即使发生了短路事件，也不致相互影响。只是这里要指出的是，使用中继器并不增加最大允许的连接从站数目。

使用扩展器可以同样实现 AS-i 电缆的扩展。这种方式下，第一个网段就不能再连接从站了，扩展器一般用在距离较长的场合，如用在控制柜和生产设备之间。

每个 AS-i 网段的最大长度是 100m。使用扩展器或中继器模块最多可将网络长度扩展到 3 个网段。图 3-8 所示为 AS-i 网络接扩展器、中继器的示例。

3）编址器、监控器。用于从站编址及网络监控。

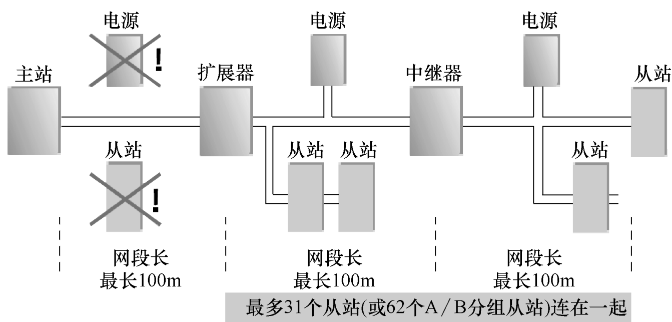


图 3-8　AS-i 网络接扩展器、中继器示例

2. AS-i 拓扑结构

AS-i 网络的拓扑结构包括总线型、星形和树形结构，可以完全适应各种工业场合。图 3-9 所示即为它的拓扑结构。

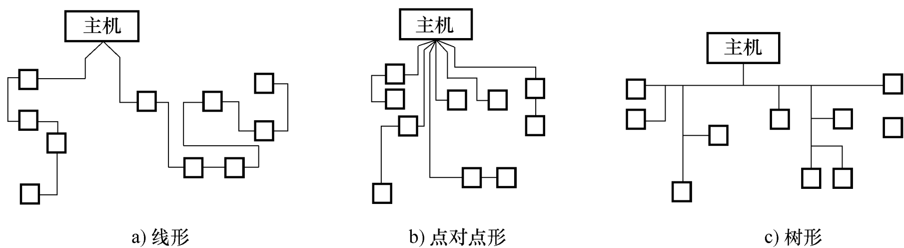


图 3-9　AS-i 拓扑结构

3. AS-i 网络模型

AS-i 为主从网络，其网络模型比较简单，仅 4 层，即物理层、传输控制层、执行控制层及主机接口层。其各层的功能及其与 ISO/OSI 参考模型的对应关系见表 3-3。

表 3-3　AS-i 各层功能及其与 ISO/OSI 参考模型对应关系

名　　称	功　　能	对应的 ISO/OSI 参考模型
主机接口层	主机接口，面向操作者	应用层
执行控制层	处理控制信息，自动地址分配	网络层
传输控制层	数据报文传输管理	数据链路层
传输物理层	收发脉冲的监控	物理层

1）物理层。物理层是面向硬件的，规定用两根导线既传递数据又提供电源，是连接网络系统中主站、从站、电源、控制器、传感器/执行器的通路。

报文信号在传输系统中要经过多次的变换和恢复，并要抵抗各种外界的干扰以保证准确、快捷、可靠的信息交换。为产生 AS-i 报文，要先将报文内容转化为不归零码（NRZ），接着转换为差动曼彻斯特码（M-Ⅱ），最后为增强抗干扰的能力，还要将 M-Ⅱ码经交变脉冲调制（Alternating pulse modulation，APM）转换为正弦平方脉冲（$\sin^2$）。具体是，在 Manchester 码的电平发生上跳变时产生一个正向正弦二次方脉冲，下跳变时产生一个负向正弦二次方脉冲，解耦装置在最后把电流信号转换成所有装置都能接收的电压信号。当电流通过解耦装置内的电感元件时会产生电压突变，增加的电流产生负向电压信号，减小的电流产生正向电压信号。图 3-10 所示为它的信号转换实例。

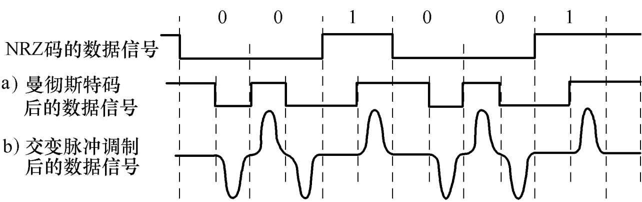


图 3-10　AS-i 信号转换实例

这里使用的 APM 信号的特点是：APM 变换后的信号是交流信号，这对于在两根电缆上同时传输电源和数据来说是必须的；用 $\sin^2$ 脉冲代替矩形方波脉冲，频谱较窄，减小了电缆终端的反射，提高了抗干扰的能力；M-Ⅱ编码自带时钟，简化了时钟恢复，不必专设一条时钟线。

ASI 总线的总传输速率为 167Kbit/s。允许的网络传输速率为 53.3Kbit/s，传输效率为 32%。

2）传输控制层。在 AS-i 网络中，每次通信都是主站发起，从站响应。主站收到响应报文后，再访问下一站点。这样过程周而复始，轮询每个从站。具体报文由主站请求、主站暂停、从站响应和从站暂停四个部分组成，如图 3-11 所示。

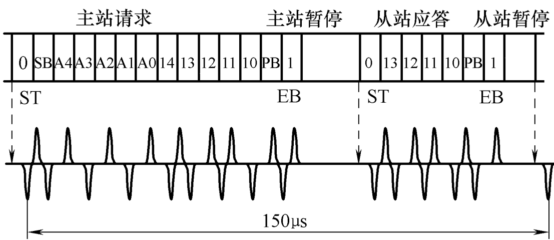


图 3-11　AS-i 传输的报文

从图知，它的所有的主站请求都是固定的 14bit 的长度，所有的从站响应的长度都是 7bit。每比特的时间是统一的 6μs。主站请求部分含义见表 3-4。

表 3-4　主站请求部分含义

数　据　位	语　　义	注　　释
ST	起始位	主站请求的起始位标志;通常为 0
CB	控制位	信息单元中数据/参数传输标志; 0 = 数据/参数传输/地址分配 1 = 命令传输
A4 ~ A0	地址位(5 位)	从站编址:0 ×00 = “0”地址 0 ×01 ~0 ×1F = 从站地址 1 ~31
I4 ~ I0	信息位	这 5 位包括对于各个请求类型传输到从站的信息

（续）

数 据 位	语 义	注 释
PB	奇偶校验位	从站对主站请求的校验 主站请求是偶校验 0 = 在(CB,A4 ~ A0,I4 ~ I0)中“1”的总数为偶数 1 = 在(CB,A4 ~ A0,I4 ~ I0)中“1”的总数为奇数
EB	结束位	主站请求结束标志

从站响应含义见表 3-5。

表 3-5 从站响应含义

数 据 位	语 义	注 释
ST	起始位	从站响应开始标志
I3 ~ I0	信息位	从站响应信息
PB	奇偶校验位	主站对从站响应校验 从站响应是偶校验 0 = 在(I3 ~ I0)中“1”的总数为偶数 1 = 在(I3 ~ I0)中“1”的总数为奇数
EB	结束位	从站响应结束标志

在 AS-i 中，主站的请求报文共有 9 种，其名称和内容见表 3-6。具体内容说明如下：

表 3-6 主站 9 种请求报文的名称和内容

报文名称	主站报文内容												
	ST	SB	5 位地址					5 位参数					PB	EB
数据交换	0	0	A4	A3	A2	A1	A0	0	D3	D2	D1	D0	PB	1
写参数	0	0	A4	A3	A2	A1	A0	1	D3	D2	D1	D0	PB	1
地址分配	0	0	0	0	0	0	0	A4	A3	A2	A1	A0	PB	1
复位	0	1	A4	A3	A2	A1	A0	1	1	1	0	0	PB	1
删除操作地址	0	1	A4	A3	A2	A1	A0	0	0	0	0	0	PB	1
读 I/O 配置	0	1	A4	A3	A2	A1	A0	1	0	0	0	0	PB	1
读 ID 编码	0	1	A4	A3	A2	A1	A0	1	0	0	0	1	PB	1
状态读取	0	1	A4	A3	A2	A1	A0	1	1	1	1	0	PB	1
读出状态和状态删除	0	1	A4	A3	A2	A1	A0	1	1	1	1	1	PB	1

① 数据交换。要求从站把测量数据上传给主站，而主站又可以把控制指令下达给从站。

② 写参数。设置从站功能，如传感器的测量范围、激活定时器、在多传感器系统中改变测量方法等。

③ 地址分配。只有当从站地址为 00H 时才有效。从站接到这个请求后，用 06H 回答，表示已收到了主站的正确请求，从站从此就可以在这个新地址被呼叫了，同时把这个新地址存储在从站的 EEPROM 中，这个过程大约需要 15ms。这种方式使主站可以对运行中损坏后重新置换的从站自动进行原有地址的设置。

④ 复位。把被呼叫的从站地址恢复到初始状态，从站用 06H 回答，整个过程需 2ms。

⑤ 删除操作地址。暂时把被呼叫的从站地址改为 00H，这个报文一般和“地址分配”报文一起使用。当新地址确定后，从站用 06H 回答。如果使用指令“Reset-ASI-Slave”就可以恢复原地址。

⑥ 读 I/O 配置。

⑦ 读 ID 编码。从站的 I/O 设置和 ID 编码在出厂时已经确定，不能改变。⑥、⑦结合使用的目的是确定从站的身份。

⑧ 状态读取。读取从站状态缓冲器中的 4 个数据位，以获得在寻址和复位过程中出现的错误信息。

⑨ 读出状态和状态删除。读出从站状态缓冲器的内容，然后删除。

在以上 9 种主站请求报文中，用户最常用的就是数据交换报文了。

3）执行控制层。用以完成主站和从站之间的数据交换。主站有两种运行模式：

① 配置模式。在此模式下，无须与参考配置进行核对，都可与从站通信。

② 运行保护模式。在此模式下，主站将只与“激活从机列表（LAS）”中的从站通信，并对 AS-i 的配置进行自动测试。只有位于“从机列表（LPS）”中，其实际配置与参考配置又相一致的从机才能被激活。此时可以进行自动地址设定。若发现差错，将向“主站接口层”报告差错信息。

此外，2.1 版本的技术标准为了将每个主站所能控制的最大从站个数由原来的 31 个增加到 62 个，且保持对已有旧版本的兼容性，引入了所谓的“扩展地址模式”，即对于遵照新标准生产的 ID 码为“HEXE”的从站设备，每个主站最多可以控制 62 个这样的从站。

要将从站个数翻倍，这必然要求地址位要多出一位，但又要保持对旧版本系统的兼容性，所以新版本技术规范规定，在主站请求报文中保持原来的 5 位地址位不变，添加 1 位新的选择位，该位占用主站请求报文中信息位的第二位。用它可将连接在主站上的从站分为 A/B 两组，每组最多为 31 个。这意味着在 2.1 版本“扩展地址模式”下，主站请求报文中信息位比原来少了一位。原来的信息位共有 5 位，其中有 4 位是给从站的信息，而在地址扩展模式下，给从站的信息则相应减少了一位，变成了 3 位。所以，在新版本的扩展地址模式下，主站发给从站的有效数据最多为 3 位，最多只有 3 个输出。

由于地址的扩充不涉及从站响应消息，所以从站应答消息的结构在新技术规范中仍保持不变，输入最多数据仍然是 4 位。

引入所谓的“扩展地址模式”，每个地址可连接 2 个从站（分为 A/B 组），如：地址为 10A 或 10B。I/O 端口数从 124(31×4)I+124(31×4)O(2.0 版本）扩展到 248（62×4)I+186(62×3)O(2.1 版本)。

在一个周期中先扫描 A 组从站，再扫描 B 组从站，所以总线最大周期由原来的 5ms 翻倍变为 10ms。

在具体选用时，可以单用 A 或 B 中的一组，也可以 A/B 组混用。唯一的变化为主站请求报文中信息的第 9 位为 1 则定义为 A 组，0 则定义与 B 组。这第 9 位如图 3-12 中标有黑点所示。

4）应用层。定义了 AS-i 的命令格式、数据内容、AS-i 周期的顺序以及主站和从站的行为。

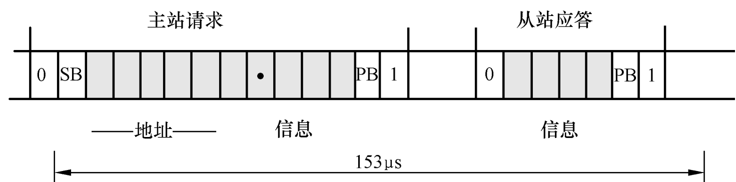


图 3-12 AS-i 总线 2.1 版本报文格式

4. AS-i 网络模拟量传输问题

AS-i 总线每次只能向从站发送 4 位的控制数据和得到从站应答的 4 位响应数据。传送的模拟量数据一般都多于 4 位（如 16 位分辨率的模拟量数据），所以，传送模拟量要将其分割成各分片，逐片传送。接收方收到分片后，重组这些分片，再恢复模拟量原值。旧版本的这些工作用 PLC 程序实现，使用起来很不方便。

在版本（2.1 版本）AS-i 中，对此作了改进。将分片和重组的功能集成给站点硬件，由硬件完成。它的技术规范还制定了模拟量从站行规（Slave-Profile7.3 和 Slave-Profile7.4），统一规定了从站的技术细节。这样，AS-i 主站就能够自动识别出所谓的“模拟量从站”，并做出相应的反应。

其实没有必要了解太多关于模拟量传送过程中的细节，但要记住的是：

1）根据 AS-i 从站行规 7.3，每个从站（I/O 模块）最多可以连续传送 4 路模拟量信号，由于传输方法的限制，所有模拟量的从站不能使用 2.1 版本技术规范中的扩展地址模式，即一个模拟量从站只能分配给 1 ~ 31 中的一个地址。一个 AS-i 总线网络在带有模拟量从站时，总的容量就介于 1 个模拟量从站（4 路模拟量信号，4 × 1 = 4）加 60 个开关量从站和 31 个模拟量从站（124 路模拟量信号，4 × 31 = 124）但不带有开关量从站。

2）AS-i 从站行规 7.3 规定每个模拟量信号有 16 位有效数据，分为 7 个分片传送，每传送一个模拟量信号需要 7 个 AS-i 总线周期，约为 70ms。

3）在 AS-i 从站行规 7.4 中规定的在模拟量非周期传输中，更加丰富了模拟量从站的功能，模拟量从站的参数可以多达 219 字节，它描述了从站不同的功能。主站通过模拟量的非周期传输可向从站设置不同的参数，每次可传送 4 位信息量，用来规定模拟量数值范围即改变量程等。

5. AS-i 主要特点

1）AS-i 传输数据量少，数据帧长度是固定的。通信周期相对固定。对 31 个站点从站最大为 5ms，对 62 个站点从站最大为 10ms。所以，通信的实时性好，确定性也有保障，很适合现场控制使用。

2）AS-i 从设备硬件到软件都按照高可靠性的规范和协议进行开发和制造，可确保它的高可靠性。它有很多具体措施，如：

① 采用特殊的报文编码和信号传输方式，数据传输安全可靠；

② 使用冗余校验，可检测到传送过程出现的差错；

③ AS-i 网络系统设计成对称结构，从而将电磁干扰降到最小；

④ 主、从站采用专用集成电路 IC 制造，比用分离元件更可靠；

⑤ 主站可连续监控网络运行、从站工作状况；

⑥ 从站能自我监控，可报告运行错误；

⑦ 使用扁平电缆的“穿刺技术”连线，可使网络施工故障大大减少。

等等。

3）AS-i网络组建，安装、使用方便，是一个能够自动完成各种配置的系统。维修也方便，一旦某个AS-i从站发生故障，它也很容易用一个新的（地址为0）同样型号的从站模块来替代。之后，主站会自动给更换的新从站赋址，把故障模块原地址自动写入到新模块中。AS-i总线支持带电拔插功能。AS-i系统简单，用户不需要进行任何的设置或调节。

4）AS-i总线是一个开放的系统，ASI国际协会对AS-i总线技术制订了详细的规范、附件和试验技术规则，便于更多产品入网。为它的应用与发展提供了很多有利条件。

5）AS-i处于PLC网络的最底层，AS-i主站可以看做是智能型传感器/执行器和控制器之间的接口。对上可与控制器或高层网络的网关相连，对下直对远程现场设备。具有现场总线所具有的优势，也是PLC实施远程控制最经济的解决方案之一。有人对某个系统做过论证，使用AS-i与传统的布线技术相比，可节省26.6%的费用。具体分析如图3-13所示。

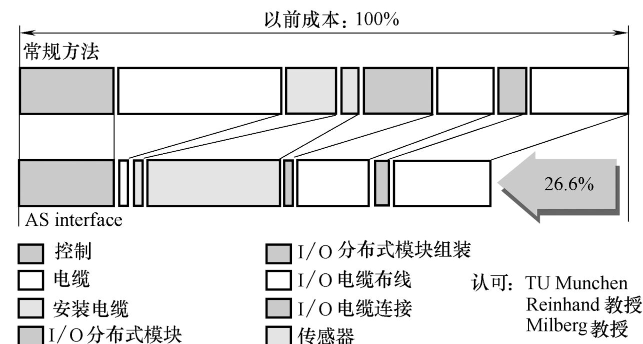


图3-13　AS-i效益图示

AS-i的问题是，从站多不具备自身控制功能。从分散风险的角度看，它还不是真正意义上的网络。再就是处理模拟量延时较长，不是它的擅长。

3.2.2　西门子PLC AS-i网络组件

1. 西门子PLC AS-i组件

西门子公司的AS-i产品齐全，其组件有主站、从站、电源及附件等。甚至还可提供分散化的驱动，如接触器的就地控制、电机起动器等。

（1）主站

S7-200的CP243-2、S7-300的CP342-2及CP342-2P的AS-i主站模块，可与S7-200、S7-300的CPU一起作为AS-i主站。还有AT短卡CP2413，可安装在计算机上，并使用西门子提供适应于MS-DOS、Microsoft Windows 3.1和Windows 95/NT操作系统的相关驱动软件，计算机也可以当作AS-i的主站。只是这个短卡除了可对网络做些设定及测试，实际用处不大。

此外，还有Profibus（DP/ASILINK）及以太网（IE/ASILINK）到AS-i的网关模块，也可作为AS-i的主站。可使用这个网关，把AS-i的从站接入Profibus网或以太网。

1）S7-200主站。要安装CP243-2模块，可同时支持2.1、2.0版本。CP243-2模块面板外观，如图3-14所示。

从图知，其上有电缆连接器，可用于连接电源及接地。还有设定按钮、显示按钮，可用

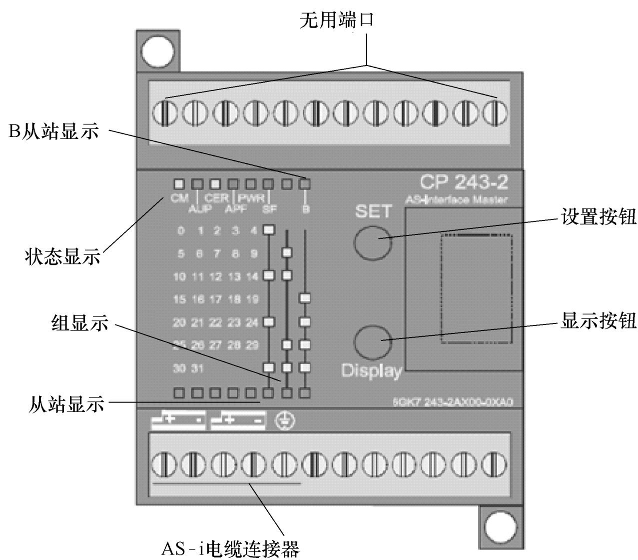


图 3-14　CP243-2 模块面板外观

于网络工作模式设置及显示选择。此外还有从站显示、从站组显示及 B 从站显示，可显示模块状态及从站地址。

状态指示灯有 6 个。其功能见表 3-7。

表 3-7　状态指示灯功能

指　示　灯	状　　态	意　　义
CM(黄)	组态模式	灯亮处于组态模式,反之处于保护模式。通过 CP243-2 识别从站时,选择组态模式在该模式下,CP 激活所有 ASI 从站并进行数据交换
AUP(绿)	自动编程	在保护模式下,显示可以为替换的 ASI 从站进行自动编址
CER(黄)	组态错误	灯亮,表示从站组态与实际设置不匹配
APF(红)	电源错误	电源供电无效或电压过低
PWR(绿)	电源	
SF(红)	系统错误	点亮表示有内部错误;或按钮按下时,不能改变当前模式

从站地址显示有两种模式：保护模式，只显示已组态并已激活的从站地址；配置模式，显示所有从站地址。具体地址是分组显示的，每组只显示 5 个可能存在的地址，并与 5 个从站显示灯对应。如果 5 个指示灯全亮，则表明这 5 个从站都已存在。至于显示的是哪个组，则由显示按钮选择，并通过“从站组显示”的 3 个显示灯按二进制编码确定。

上电时缺省显示为状态显示。这时，按压一次显示按钮，则状态除显示电源外其他不予显示，并转为显示从站地址。先是第 1 组地址，再按压显示按钮一次，转为第 2 组地址，依次类推。直到最后一组，即第 7 组显示时，再按压显示按钮一次，又回到状态显示。如果又继续按压显示按钮，则重复上述过程。

出厂时，从站缺省地址为 0。网络组态时，要对其进行地址分配。网络中所有从站地址应是唯一的。分配地址可以使用地址分配器，也可用软件分配。软件分配时每次只能针对一个未分配地址的从站。多个从站应依次分配，否则将出错。但已分配地址的从站，如果其中仅有一个出现故障，更换新模块（地址为 0）后，主站可自动对其编址（设定为原来地址）。

2）通信过程。实际通信有两个过程，CP243-2 与各个从站及 CPU 与 CP243-2，如图 3-15所示。前者是自动通信，有关数据存放在 CP243-2 存放在 I/O 区、CPU 特殊寄存器及模块其本身的海量存储区中；后者通信是要由用户程序访问上述 I/O 区、CPU 特殊寄存器及 CP243-2 海量存储区实现。

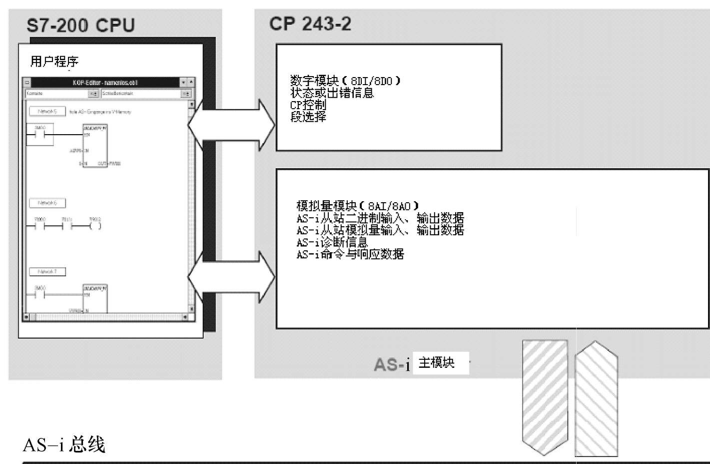


图 3-15　通信过程示意

在一个 S7-200 上，最多只能安装两个 CP243-2 模块。每个模块要占用若干个 CPU 特殊寄存器（SMB8 ~ SMB21 中的 4 字节），还要占用 I/O 区。这 I/O 区除了各 8 位的 DI、DQ，还有各 8 个字的 AI、AQ。具体地址以及占用哪个特殊寄存器与模块安装的位置及 CPU 的型号有关。如 CPU222，CP243-2 模块安装在紧接 CPU 处，则占用特殊寄存器为 SMB8、9（与开关量扩展模块对应）及 SMB10、11（与模拟量扩展模块对应）。占用开关量地址为 8 位 DI（I0.0 ~ I1.7）、8 位 DO（Q0.0 ~ Q0.7）。占用模拟量地址为 8 字 AI（AIW0 到 AIW14）、8 字 AO（AQW0 ~ AQW14）。

这里的 SMB8、SM10 为开关量模块识别寄存器，SMB9、SM11 为模块出错记录寄存器。前者标记着模块类型、I/O 类型、输入和输出点数；后者为对相应模块所测得的 I/O 出错提示。这些与 S7-200 其他扩展模块使用的寄存器类似，只是它要占用 4 字节。

这里的 8 位 DI 各位的含义为：位 0 为 ASI_MODE；位 1 为 CP_READY；位 6 为 ASI_RESP；其余均为 0。具体取值含义见表 3-8。

表 3-8　DI 各位含义

位	值	含　义
ASI_MODE	0	CP 234-2 处保护模式
	1	CP 234-2 处组态模式
CP_READY	0	电源接通 CP 234-2 未运行
	1	CP 234-2 运行
ASI_RESP	0/1	AS-i 命令接口响应位

这里的 8 位 DO 各位的含义为：位 6 为 ASI_COM；位 7 为 PLC_RUN；位 0 ~ 位 5 为段选择位。具体取值含义见表 3-9。

表 3-9 DO 各位含义

位	值	含　　义
BS0 ~ BS5	0 ~ 63	模拟量模块段选择位
ASI_COM	0/1	AS-i 命令接口作业位
PLC-RUN	在 S7-200 停止模式,须发送定义值到各个从站 由于 AS-i 从站数据是通过模拟量区传送,而当 S7-200 从运行转为停止时,又未对这个区清零,故必须用以下 PLC_RUN 位,指定此值	
	0	给 CP 243-2 指明 S7-200 处停止模式 CP 243-2 发送“0”AS-i 位从站。而模拟量值则终止传送模拟量输出从站。当 S7-200CPU 有运行转为停止时,这个位自动设为 0
	1	给 CP 243-2 指明 S7-200 处运行模式 CP 243-2 发送输出段 0 的内容给 AS-i 所有从站。在第一扫描周期,用户程序必须设此位为 1。但不要用 S7-200 的 CPU 组态输出或强制输出使这个位置 1(常处于 1 状态)

这里的各 8 个字的 AI、AQ 指的不只是这 8 个字本身，而是代表 CP243-2 模块海量缓冲区（buffer）。这个存储区是以段（Bank）划分。有输入、输出各 64 段（bank0 ~ bank63），每段有 8 个字、16 字节。各段有各段的功能。如通信命令响应数据则存放于输入段 bank2 中，通信命令数据则存放于输出段 bank2 中。具体各段的功能示意如图 3-16 所示。使用它时，要先指定段号，然后再访问。而且一般讲，要以段为单位访问。

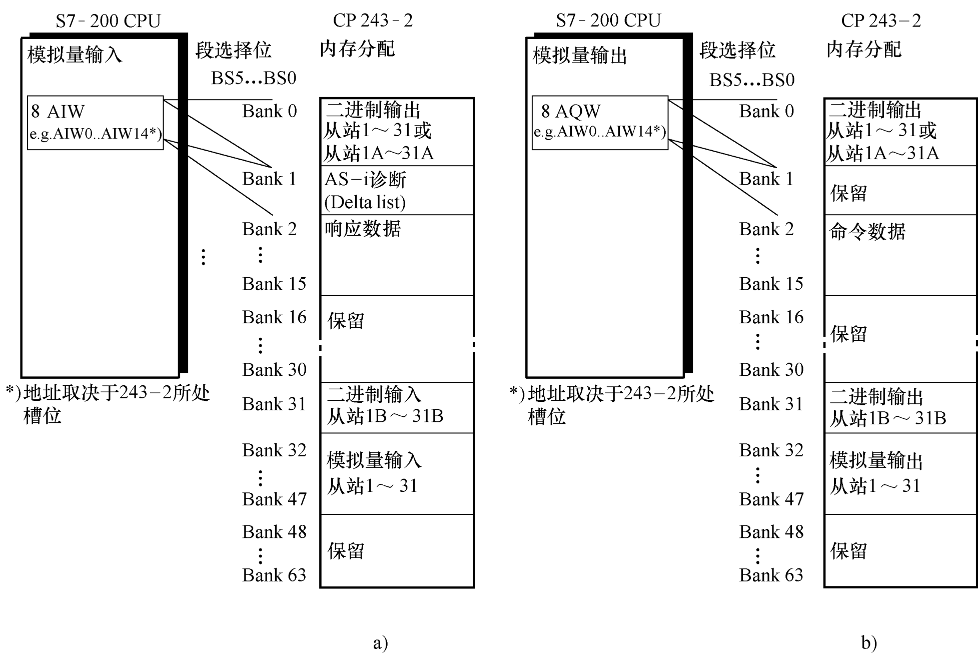


图 3-16　各段的功能示意

输入 bank0 用于存放地址 1 ~ 31 或 1A ~ 31A 从站的开关量输入。表 3-10 所示即为从站地址与输入位的对应关系。表每个从站占据 4 位，m 为 AI 的起始地址。

输出 bank0，用于存放地址 1 ~ 31 或 1A ~ 31A 从站的开关量输出。表 3-11 所示即为从站地址与输出位的对应关系。表中每个从站也占据 4 位，n 为 AQ 的起始地址。

表 3-10　从站地址与输入位对应关系

段	位号	位 7 ~ 4	位 3 ~ 0
0	$m+0$	保留	从站 1 或从站 1A 位 3　位 2　位 1　位 0
0	$m+1$	从站 2 或从站 2A	从站 3 或从站 3A
0	$m+2$	从站 4 或从站 4A	从站 5 或从站 5A
0	$m+3$	从站 6 或从站 6A	从站 2 或从站 7A
0	$m+4$	从站 8 或从站 8A	从站 2 或从站 9A
0	$m+5$	从站 10 或从站 10A	从站 2 或从站 11A
0	$m+6$	从站 12 或从站 12A	从站 2 或从站 13A
0	$m+7$	从站 14 或从站 14A	从站 3 或从站 15A
0	$m+8$	从站 16 或从站 16A	从站 2 或从站 17A
0	$m+9$	从站 18 或从站 18A	从站 2 或从站 19A
0	$m+10$	从站 20 或从站 20A	从站 2 或从站 21A
0	$m+11$	从站 22 或从站 22A	从站 2 或从站 23A
0	$m+12$	从站 24 或从站 24A	从站 2 或从站 25A
0	$m+13$	从站 26 或从站 26A	从站 3 或从站 27A
0	$m+14$	从站 28 或从站 28A	从站 2 或从站 29A
0	$m+15$	从站 30 或从站 30A 位 3　位 2　位 1　位 0	从站 31 或从站 31A 位 3　位 2　位 1　位 0

表 3-11　从站地址与输出位对应关系

段	位号	位 7 ~ 4	位 3 ~ 0
0	$n+0$	保留	从站 1 或从站 1A 位 3　位 2　位 1　位 0
0	$n+1$	从站 2 或从站 2A	从站 3 或从站 3A
0	$n+2$	从站 4 或从站 4A	从站 5 或从站 5A
0	$n+3$	从站 6 或从站 6A	从站 2 或从站 7A
0	$n+4$	从站 8 或从站 8A	从站 2 或从站 9A
0	$n+5$	从站 10 或从站 10A	从站 2 或从站 11A
0	$n+6$	从站 12 或从站 12A	从站 2 或从站 13A
0	$n+7$	从站 14 或从站 14A	从站 3 或从站 15A
0	$n+8$	从站 16 或从站 16A	从站 2 或从站 17A
0	$n+9$	从站 18 或从站 18A	从站 2 或从站 19A
0	$n+10$	从站 20 或从站 20A	从站 2 或从站 21A
0	$n+11$	从站 22 或从站 22A	从站 2 或从站 23A
0	$n+12$	从站 24 或从站 24A	从站 2 或从站 25A
0	$n+13$	从站 26 或从站 26A	从站 3 或从站 27A
0	$n+14$	从站 28 或从站 28A	从站 2 或从站 29A
0	$n+15$	从站 30 或从站 30A 位 3　位 2　位 1　位 0	从站 31 或从站 31A 位 3　位 2　位 1　位 0

弄清 CP243-2 与从站通信数据存放的位置，就便于编写用户程序，并通过执行这个程序访问这些数据。具体通信过程见将要介绍的应用实例。

要提醒的是在通信之前要求注意的事项有 4 点：

① 当使用 CP243-2 模块时，必须禁止 PLC 中的模拟量滤波。如果不禁止 PLC 中的模拟量滤波，则会破坏数字点数据，而且出错条件也不会在模拟量控制字中以位的状态来返回。

② 程序运行开始第一扫描周期，必须置“PLC_RUN”位（位 7）为“1”。

③ 仅仅当数据状态字节第 1 位，即“CP_Ready”位为“ON”时，才可读取各从站数据。

④ 当 PLC 处于停机模式时，“PLC_RUN”位自动变为“0”，其结果将是从站开关量输出不为“0”。

3）S7-300 主站。可使用 CP343-2、CP343-2P 两种模块。两者功能基本相同，但 CP343-2P 版本新，在配置上有更多的选择。这两种模块可安装在 S7-300 机架上，也可安装在 Profibus 的从站 ET-200M 机架上。安装后要各占用 16 个模拟量输入、输出字节。图 3-17 所示为其外观。

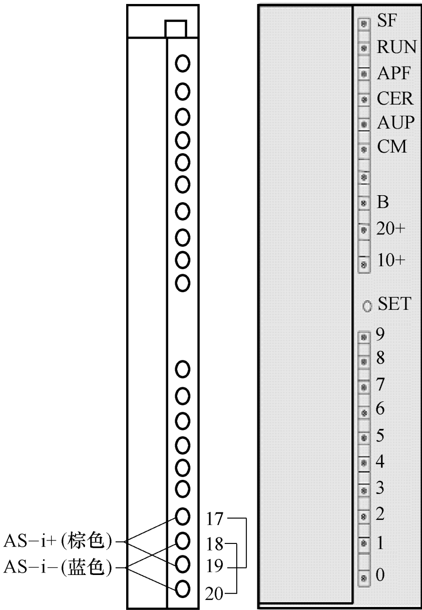


图 3-17　CP343-2、CP343-2P 模块外观

其上指示灯含义见表 3-12。

表 3-12　CP343-2、CP343-2P 模块指示灯含义

LED	意　　义
SF	系统错误。该灯亮表明系统在保护模式下 ASI 系统发生故障(如从站错误等)
RUN	显示 CP 正常启动
APF	ASI 电源错误
CER	组态错误。下列情况中 CER 点亮： • 组态的从站在 ASI 网络上不存在 • 网络上的从站未被组态 • 从站实际数据与 CP 中的组态数据不匹配 • CP 处于离线状态
AUP	可以自动编程(CP 出于保护模式)
CM	组态模式 在组态模式下,CP 可与连接在 ASI 电缆上的各个站点交换数据(除站地址为 0 的从站),新添加到电缆上的从站可以立即被主站识别 安装和运行完成后,可以通过 SET 按钮,将 CP 转换为保护模式。在保护模式下,CP 只与组态过的从站进行数据交换

其实际通信也是两个过程，CP343 与各个从站及 CPU 与 CP343。前者是自动通信，有关数据存放在 CP34 存放在 I/O 区中；后者通信要由用户程序使用 I/O 命令访问上述 I/O 区。这个 I/O 区及有关从站可以用 STEP7 编程软件配置。有关细节可参阅 CP323 说明书。

4）接入 Profibus 的 DP/ASILINK 模块及接入以太网 IE/ASILINK 模块。用它作为网关，可使 AS-i 网络连接到 Profibus-DP，或连接到西门子以太网。该网关具有 IP20、IP65 的保护

等级。在 AS-i 网络它为主站，而在 PROFIBUS、以太网它则作为从站。例如通过这种方式 SIMATICS7-400 自动化系统可以连接到 AS-i 中。如果用于 PROFIBUS 网络的分布式 I/O 系统，SIMATIC ET200X 也可以通过一个特殊通信处理器借助一个双端连接器连接到 AS-i。

（2）从站

从站模块有安装在控制柜里的与安装在现场的。

1）安装在控制柜里的从站，产品较多。

有 IP20 的保护等级的线条型模块。用于连接普通 I/O 点。可以安装在控制柜里实现紧凑的分布式的配置。该模块可以像其他低压设备一样安装在 DIN 导轨上或用螺钉固定在控制柜的背板上。

还有负荷馈电模块。也就是一些智能的电机启动器、控制器。其控制电路可以完全预先连接到 AS-i 的负荷馈电模块上。其反馈信号都可以在输入模块上。而输出模块则可用于对接触器线圈的直接控制。

再就是 LOGO 微型控制器。它是第一个智能化的 AS-i 从站。有了它就可以直接在机器上实现小型的分布式自动化控制任务。LOGO 提供了完成这些任务的集成的基本和特殊的功能。例如：AND、OR、NAND、NOR、ON/OFF 继电器、时钟发生器、计数器、时间开关等等。这样一来实现分布式的自动化任务和设备的扩展都是非常容易的。如果 AS-i 主站或总线上出现了故障，它仍然能够继续独立工作，因为它自带电源。主站和智能型从站的组合为建立小型的，分布广泛的车间结构提供了新的可能性。

2）安装在现场的 AS-i 从站（I/O 模块），产品也较多。

有结构紧凑型模块。这是一种具有较高保护等级的新一代紧凑型 AS-i 模块。包括数字、模拟、气动和 24V 直流电机起动器模块。模块具有两种尺寸：K45 和 K60，可以满足各种安装要求。每个模拟量模块有两个通道，模块又可以分成 5 种类型：电流型传感器输入模块、电压型传感器输入模块、热电阻型传感器输入模块、电流型执行器输出模块、电压型执行器输出模块。

有气动控制模块。通过一个集成的编址插孔可以对已经安装的模块编址。用一个可选的保护罩将编址插孔密封起来，其保护度为 IP67。LED 显示装置可以进行即时诊断。作为一种特殊的选择，西门子提供了可以连接模拟量的模块。所有的模块都可以通过 SIMATIC S7 系列的可编程序控制器进行通信的参数预置。

有负荷馈电模块。可以直接连到电机上，采用相同的方法 AS-i 气动模块的阀门也可以直接连到汽缸上。这意味着作为气动单元输出的阀门和来源于汽缸的位置信号现在可以组合到同一个模块上。西门子提供两种类型的气动模块：带两个集成的 3/2 路阀门的气动用户模块和带两个集成的 4/2 路阀门的气动紧凑型模块。气动紧凑型模块有单稳和双稳两种类型。

有交流电机起动器。AS-i 电机起动器是装于封闭外壳内的直接或可逆起动器，控制功率达 4kW。由于使用坚固的金属外壳，其保护度可以达到 IP65。内部非熔断器保护的负载馈电器为 SIRIUS3R 开关装置。AS-i 数据电缆和 DC 24V 辅助电源线通过绝缘穿刺技术可直接连接到电源上。AS-i 电机起动器可通过金属外壳后板上的安装孔固定。

有 DC 24V 电机起动器。采用 DC K60AS-i24V 电机起动器可以实现 70W 功率的拖动，即在同一台设备上将 DC 24V 电机起动器及其传感器直接连接到 AS-i 上。有 3 种不同型号的电机起动器：直接起动器（不带制动器和和可选的急停功能），双直接起动器（带制动器和可选的急停功能），可逆起动器（带制动器及可选的急停功能）。

有紧凑型起动器。具有 IP65 的保护等级，已经实现了与负荷馈电模块的内部预接线。并且对任何 5.5kW 及以下三相电流负载 AC 400/500V 实现开关和保护，即通常三相标准电机的直接和可逆操作。其内部安装有机电式开关组件或电子式过载保护及断路器（后者最大控制功率 2.2kW）。AS-i 紧凑型起动器也可在接线完成后编址。

有电子电动机控制单元。SIKOSTART®电子电动机控制单元适合用来控制电动机的软起动和软停止操作，及三相感应式电机的制动和节能操作。例如它可以应用在对工具机械、传送带、风扇、压缩机及泵的控制上。AS-i 控制模块可以安装在任何设备上，用以实现对设备的控制（起动和停止）和接收其继电器反馈的状态信号。

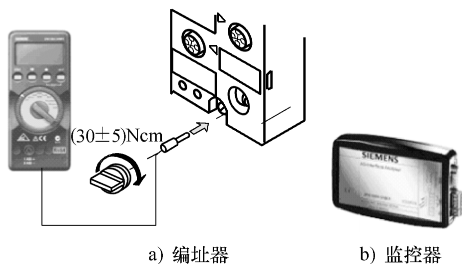
有集成 AS-i 芯片的接近开关。BERO 接近开关可以直接连接到执行器-传感器接口或接口模块上。特殊的感应式、光学和声纳 BERO 接近开关适合直接连接到执行器—传感器接口上。除了开关输出之外，它们的显著特点是集成有 AS-i 芯片，还提供其他信息（例如，开关范围和线圈故障）。通过 AS-i 电缆可以对这些智能 BERO 设置参数。

有按钮和 LEDS。具有 AS-i 的 SIGNUM3SB3 控制设备可以实现完全的通信功能。通过集成的 AS-i 模块 4I/4O 以很少的接线就可以将其连接到 AS-i 网络系统上。带灯指令按钮通过 AS-i 电缆供电。通过特殊的 AS-i 从站和独立的辅助电源可以实现控制设备的单个连接，这样一来，每个设备可以最多连接 28 个常开触点和 7 个信号输出点。

SIGNUM3SB4 是一个具有 AS-i 接口的完整的操作员通信系统人机接界面。

最后还有 AS-i 安全产品（ASIsafe）。这些包括紧急制动开关、光栅、保护门接触器、安全灯等。当事故发生需要保护人身安全和设备的时候，这些传感器和执行器以可靠的反馈信号不间断的在毫秒级时间范围内优先动作。

（3）其他产品，除了电源、电缆，还有编址器（Addressing unit）及监控器（Analyzer）。图 3-18a所示为编址器外观及其使用。当其与从站模块连接后，可选择相应功能，进行对从站各个站点编址；读写从站数据、参数；测量网络电压；存储所作设定等。



a) 编址器　b) 监控器

图 3-18　编址器、监控器外观

图 3-18b 所示为监控器外观。可用其检测 AS-i 网络质量与可靠性、对从站各个站点的远程分析与诊断。有关数据可通过 RS-232 接口传送还给计算机。计算机可运用相关软件对其做评估，自动生成相应报告。计算机也还可在线查看所作的分析与检测。

3.2.3　西门子 PLC AS-i 网络配置实例

1. S7-200 使用 CP243-2 模块连接 4 个从站的实例

其配置如图 3-19 所示。

这里，从站 2 为 4 个输入点，从站 3 为 2 个输入点、2 个输入点，从站 4 为 4 个输入点，从站 31 为 4 个输入点、4 个输入点。图中灰色背景为这些输入、输出点占用的地址。而白色背景的没有使用，与程序无关。

访问从站存储区数据可使用如图 3-20 所示程序。图 3-20a 为主程序。当 PLC 处运行状

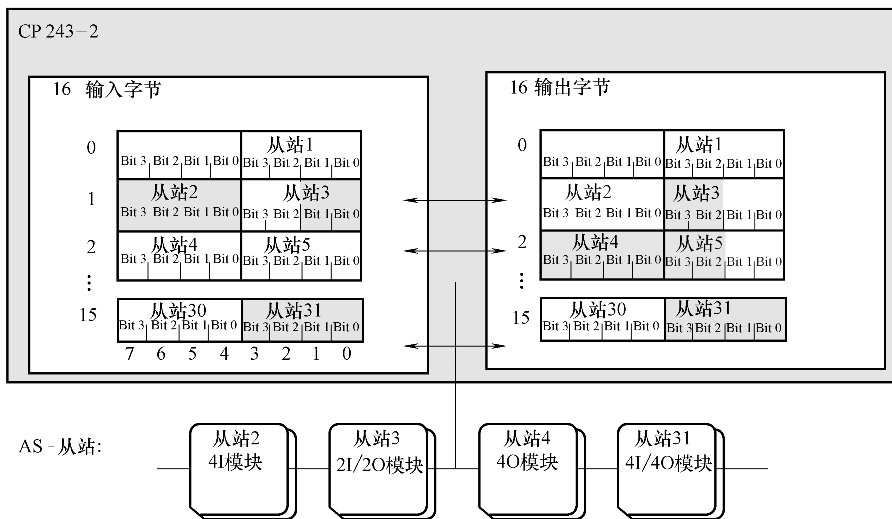


图 3-19　S7-200 使用 CP243-2 模块连接 4 个从站实例

态时，SM0.1ON 一个周期，使 Q1.7 置 1。启动 AS-i 网络工作。而当 I1.1ON 时（表明 AS-i 网络工作就绪）则调子程序（见图 3-20b）。

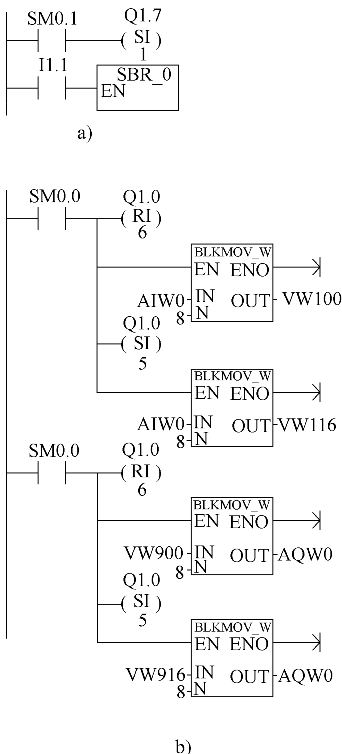


图 3-20　访问从站存储区数据程序

在子程序梯级 1 中，先是设定段 0，然后把 AIW0（这时它指的即为输入段 0 的 8 个字）全部数据传送给 VW100～VW114 的 8 个字中；后是设定段 31，然后把 AIW0（这时它指的即为段 31 的 8 个字）全部数据传送给 VW116～VW128 的 8 个字中。可知，这里前者实际是各个标准或 A 从站的全部输入数据；后者实际是各个 B 从站全部的输入数据。

在子程序梯级 2 中，先是设定段 0，然后把 VW900～VW914 各个字的数据分别传送到 AQW0（这时它指的即为输出段 0 的 8 个字）；后是设定段 31，然后把 VW916～VW928 各个字的数据分别传送到 AQW0（这时它指的即为输出段 31 的 8 个字）。可知，这里前者实际是各个标准或 A 从站的全部输出数据；后者实际是各个 B 从站全部的输出数据。

不断执行此子程序，将把 CP243-2 模块输入缓冲区段 0、31 的数据对应地反映到 VW100V～VW128 的 16 个字中。而这 VW100V～W128 的 16 个字数据可按需要按位使用。同样，也将 VW900V～W928 的 16 个字的数据对应地反映到 CP243-2 模块输出缓冲区段 0、31 中。而针对本例，与从站 2 对应的输入位为：V101.4、V101.5、V101.6、V101.7，与从站 3 对应的输入位为：V101.0、V101.1，与从站 3 对应的输出位为：V901.3、V901.4，与从站 31 对应的输入位为：V115.0、V115.1、

V115.2、V115.3，从站 31 对应的输出位为 V915.0、V915.1、V915.2、V915.3。而这些位怎么使用是实际编程工作，这里略。

实际上，西门子 S7-200 的编程软件提供有 AS-i 配置向导，可利用它做网络配置，可直接生成上述位的变量。表 3-13 所示即为与本例对应的有关变量。

表 3-13　与本例对应的有关变量

	Symbol	Address	Comment
1	DI031_1	V115.0	Symbol Input 1:Slave 31 · Digital[4I/4Q(St 7Hex)]
2	DI031_2	V115.1	Symbol Input 2:Slave 31 · Digital[4I/4Q(St 7Hex)]
3	DI031_3	V115.2	Symbol Input 3:Slave 31 · Digital[4I/4Q(St 7Hex)]
4	DI031_4	V115.3	Symbol Input 4:Slave 31 · Digital[4I/4Q(St 7Hex)]
5	DQ031_1	V131.0	Symbol Output 1:Slave 31 · Digital[4I/4Q(St 7Hex)]
6	DQ031_2	V131.1	Symbol Output 2:Slave 31 · Digital[4I/4Q(St 7Hex)]
7	DQ031_3	V131.2	Symbol Output 3:Slave 31 · Digital[4I/4Q(St 7Hex)]
8	DQ031_4	V131.3	Symbol Output 4:Slave 31 · Digital[4I/4Q(St 7Hex)]
9	DI03_3	V101.2	Symbol Input 3:Slave 3 · Digital[2I/2Q(St BHex)]
10	DI03_4	V101.3	Symbol Input 4:Slave 3 · Digital[2I/2Q(St BHex)]
11	DQ03_1	V117.0	Symbol Output 1:Slave 3 · Digital[2I/2Q(St BHex)]
12	DQ03_2	V117.1	Symbol Output 2:Slave 3 · Digital[2I/2Q(St BHex)]
13	DI02_1	V101.4	Symbol Input 1:Slave 2 · Digital[4I/0Q(St 0Hex)]
14	DI02_2	V101.5	Symbol Input 2:Slave 2 · Digital[4I/0Q(St 0Hex)]
15	DI02_3	V101.6	Symbol Input 3:Slave 2 · Digital[4I/0Q(St 0Hex)]
16	DI02_4	V101.7	Symbol Input 4:Slave 2 · Digital[4I/0Q(St 0Hex)]

这里输入位地址与上述程序例一样，输出由于上例起始地址用的是 VW900，所以与向导配置结果有所差别。

2. S7-200 使用 CP243-2 模块连接 2 个模拟量从站的实例

本例从站地址分别为 3 与 17。前者有 4 路输入，后者有 4 路输出。其相应的主程序与图 3-20a 相同。当 I1.1ON 时（表明 AS-i 网络工作就绪）则调子程序（见图 3-21）。

在子程序梯级 1 中，先是设定段 33（存放从站 3 的模拟量输入数据），然后把 AIW0（这时它指的即为输入段 0 的 8 个字）全部数据传送给 VW100 ~ VW114 的 8 个字中。接着设定段 40，然后把 VW200 ~ VW214 各个字的数据分别传送到 AQW0（存放从站 17 的模拟量输出数据）。

不断执行此子程序，将把 CP243-2 模块输入缓冲

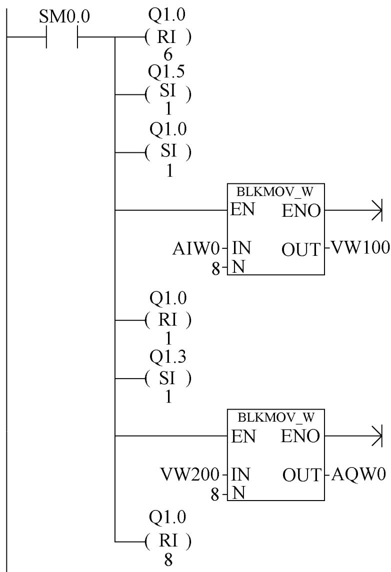


图 3-21　访问模拟量从站存储区数据子程序

区段 33 的数据对应地反映到 VW100V ~ VW114 的 8 个字中。而这 VW100 ~ VW114 的 8 个字数据可按需要使用。同样，也将 VW200 ~ VW214 的 8 个字的数据对应地反映到 CP243-2 模块输出缓冲区段 40 中。而针对本例，与从站 3 对应的输入字为：VW100、VW102、VW104、VW106、VW108、VW110、VW112、VW114。与从站 17 对应的输出字为：VW200、VW202、VW204、VW206、VW208、VW210、VW212、VW214。而这些字怎么使用是实际编程工作，这里略。

当然，也可用西门子 S7-200 的编程软件提供有 AS-i 配置向导做这个网络配置，也可直接生成上述位的变量。表 3-14 所示即为与本例对应的有关变量。

表 3-14　与本例对应的模拟量变量

	Symbol	Address	Comment
1	AQ017_4	VW114	Symbol channel 4:Slave 17 · Analog(Output,4 channel)
2	AQ017_3	VW112	Symbol channel 3:Slave 17 · Analog(Output,4 channel)
3	AQ017_2	VW110	Symbol channel 2:Slave 17 · Analog(Output,4 channel)
4	AQ017_1	VW108	Symbol channel 1:Slave 17 · Analog(Output,4 channel)
5	AI03_4	VW106	Symbol channel 4:Slave 3 · Analog(Input,4 channel)
6	AI03_3	VW104	Symbol channel 3:Slave 3 · Analog(Input,4 channel)
7	AI03_2	VW102	Symbol channel 2:Slave 3 · Analog(Input,4 channel)
8	AI03_1	VW100	Symbol channel 1:Slave 3 · Analog(Input,4 channel)

这里输入字地址与上述程序例一样，输出由于上例起始地址用的是 VW200，所以，与向导配置结果有所差别。

向导配置后还生成 3 个字程序。它们是：ASIx_CTRL、ASIx_WRITE 及 ASIx_READ。这里符号中的“x”为编号，可取不同的值。第 1 个子程序为通信启动程序，必须一直运行。第 2、3 为对从站读写命令。用于对从站的设定、编址或诊断。调用时要指出所用段号及存放命令码、命令参数的地址指针。一般用户可不使用它。有关命令很多，具体可参阅该模块说明书，这里略。

3.2.4　三菱 PLC AS-i 网络及其配置实例

三菱公司 PLC 多有 AS-i 主站模块，如 Q 型机就有 QJ71AS92，可用以组建 AS-i 网，实现 AS-i 从站 I/O 接入三菱 PLC。

1. 三菱 AS-i 网络特性

QJ71AS92 模块可安装在任何型别的 Q 型机基板的任何槽位上。安装数量只受 CPU 可控制的 I/O 点数限制。它与 AS-i V2.11、V.2.04 兼容。图 3-22 所示为该模块通过电缆、电源与从站连接的示意。

从图知，与新版本 AS-i 总线一样，所连网络的从站也有两组，A 组、B 组。此外。也可连接模拟量从站。主站除了与从站进行数据读写，还可处理从站地址分配，状态读取等其他工作。

图 3-23 所示为 QJ71AS92 模块正面图。其各指示灯及开关的功能见表 3-15 所示。

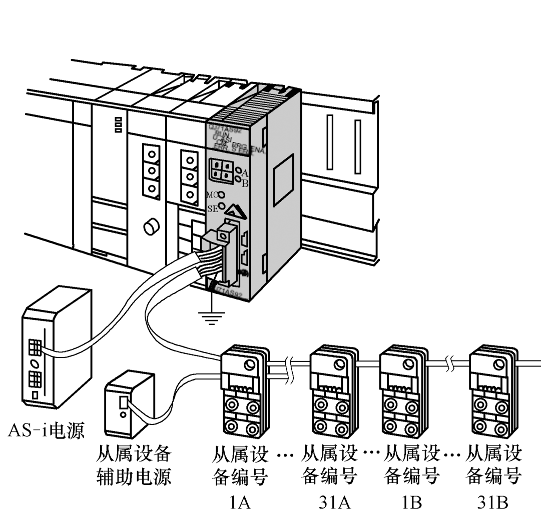


图 3-22 QJ71AS92 模块通过电缆、电源与从站连接

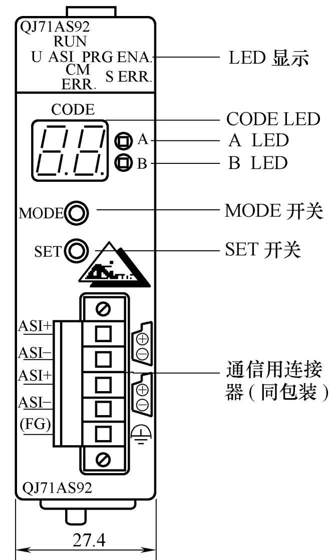


图 3-23 QJ71AS92 模块正面图

表 3-15 指示灯及开关功能说明

<table>
<tr><th>名　　称</th><th colspan="2">内　　容</th></tr>
<tr><td>CODELED</td><td colspan="2">从属设备编号,显示错误代码</td></tr>
<tr><td rowspan="6">LED 显示</td><td>RUN</td><td>亮灯:模块正常
熄灭:模块异常</td></tr>
<tr><td>U ASI</td><td>亮灯:从 AS-I 总线供电。
熄灭:不从 AS-I 总线供电</td></tr>
<tr><td>CM</td><td>亮灯:配置模式或正在存储参数
熄灭:受保护操作模式</td></tr>
<tr><td>ERR.</td><td>亮灯:检测到异常
熄灭:未检测到异常</td></tr>
<tr><td>PRG
ENA.</td><td>亮灯:从属设备编号自动分配功能处于可工作状态
熄灭:从属设备编号自动分配功能不处于可工作状态</td></tr>
<tr><td>S ERR.</td><td>—(将来用)</td></tr>
<tr><td>A　LED
B　LED</td><td colspan="2">“CODE”LED 显示从属设备编号 0～31 时,表示该从属设备的种类
<table>
<tr><th>“A”
LED</th><th>“B”
LED</th><th>内　　容</th></tr>
<tr><td>熄灭</td><td>熄灭</td><td>不分 AS-i Ver. 2. 04 I/O 从属设备,模拟从属设备和 Ver. 2. 11 系列的从属设备</td></tr>
<tr><td>亮灯</td><td>熄灭</td><td>AS-i Ver. 2. 11 A 系列 I/O 从属设备</td></tr>
<tr><td>熄灭</td><td>亮灯</td><td>AS-i Ver. 2. 11 B 系列 I/O 从属设备</td></tr>
<tr><td>亮灯</td><td>亮灯</td><td>—(将来用)</td></tr>
</table></td></tr>
<tr><td>MODE 开关</td><td colspan="2">切换受保护操作模式和配置模式</td></tr>
<tr><td>SET 开关</td><td colspan="2">给从属设备设置从属设备编号或给主模块设置参数</td></tr>
<tr><td>通信用连接器</td><td colspan="2">使用 AS-i 电缆连接 AS-i 系统</td></tr>
</table>

其主要功能与特性分别见表3-16及表3-17。

表3-16　QJ71AS92模块主要功能

项　　目	功能概要
与AS-i从属设备的通信功能	按照AS-i Ver. 2. 11的标准,可与下列从属设备连接 · AS-i Ver. 2. 11兼容的I/O从属设备 · AS-i Ver. 2. 04兼容的I/O从属设备 · AS-i Ver. 2. 11兼容的模拟从属设备
用实用程序自动刷新的功能	用实用程序包对输入输出数据的CPU软元件存储器进行自动刷新的功能
从属设备编号自动分配功能	更换从属设备时为从属编号为0的相同产品自动设置与更换前的从属设备相同的从属编号
参数设置功能	在实用程序包、模块前面板上的CODE LED和开关、梯形图程序中设置从属设备编号和参数

表3-17　QJ71AS92模块主要特性

项　　目		规　　格
AS-i系统最多从属设备数		62(A系列:31、B系列:31)
最多输入输出点数(1点=1位)	入力	248点
	出力	248点
最多模拟输入输出点数(1点=16位)	入力	124点
	出力	124点
输入输出刷新时间		约5ms(不分I/O从属设备系列)
		约10ms(分I/O从属设备系列)
		约35ms(每一通道一个从属模拟设备)
传送距离		最长100m(使用2台转发器最长可达300m)
连接形式		总线网络形式(星形、线形、树形或环形均可用)
内存		EEPROM(参数注册用)写入次数:10万次
适用电缆		使用AS-I电缆
可安装的站		Q系列CPU(Q模式)
输入输出占用点数		32点(I/O分配:智能)
DC5V内部消耗电流		0.40A
外部供电电源	电压	TYP. DC30.5V(用AS-i电源供电)
	消耗电流	46mA(TYP. DC30.5V)
外形尺寸		98(H)×27.4(W)×90(D)[mm]
重量		0.12kg

QJ71AS92模块安装在机架的某个槽位后，将占用两个输入字（X）及输出字（Y），用以读取网络状态及控制网络工作。如安装在槽位0，则所占用地址为X0～X1F，Y0～Y1F。其他位类推。这些位的含义见表3-18。显然，如果要通过用户程序读写从站数据，则必须弄清它的含义。

2. 三菱AS-i网络连接

QJ71AS92 AS-i系统连接方法有4种：星形连接、总线连接、树形连接及环形连接。如图3-24所示。连接不要求接终端器。距离超过100m要加中继器。并要在中继后接AS-i

电源。

表 3-18　QJ71AS92 模块占用输入、输出字的各个位的含义

<table>
<tr><th colspan="2">信号方向 QJ71AS92 到 PLC CPU</th><th colspan="2">信号方向 PLC CPU 到 QJ71AS92</th></tr>
<tr><th>输 入 信 号</th><th>信 号 名 称</th><th>输 出 信 号</th><th>信 号 名 称</th></tr>
<tr><td>X0</td><td>单元就绪</td><td>Y0</td><td rowspan="17">无用</td></tr>
<tr><td>X1</td><td>无用</td><td>Y1</td></tr>
<tr><td>X2</td><td>命令完成</td><td>Y2</td></tr>
<tr><td>X3</td><td>组态登记完成</td><td>Y3</td></tr>
<tr><td>X4</td><td>组态出错</td><td>Y4</td></tr>
<tr><td>X5</td><td>AS-i 电源故障</td><td>Y5</td></tr>
<tr><td>X6</td><td>正常操作确认</td><td>Y6</td></tr>
<tr><td>X7</td><td>组态模式</td><td>Y7</td></tr>
<tr><td>X8</td><td rowspan="9">无用</td><td>Y8</td></tr>
<tr><td>X9</td><td>Y9</td></tr>
<tr><td>XA</td><td>YA</td></tr>
<tr><td>XB</td><td>YB</td></tr>
<tr><td>XC</td><td>YC</td></tr>
<tr><td>XD</td><td>YD</td></tr>
<tr><td>XE</td><td>YE</td></tr>
<tr><td>XF</td><td>YF</td></tr>
<tr><td>X10</td><td>Y10</td></tr>
<tr><td>X11</td><td rowspan="15"></td><td>Y11</td><td></td></tr>
<tr><td>X12</td><td>Y12</td><td>命令要求</td></tr>
<tr><td>X13</td><td>Y13</td><td>组态登记</td></tr>
<tr><td>X14</td><td>Y14</td><td>离线</td></tr>
<tr><td>X15</td><td>Y15</td><td>从站地址自动分配</td></tr>
<tr><td>X16</td><td>Y16</td><td>组态模式</td></tr>
<tr><td>X17</td><td>Y17</td><td>保护操作模式</td></tr>
<tr><td>X18</td><td>Y18</td><td rowspan="4">无用</td></tr>
<tr><td>X19</td><td>Y19</td></tr>
<tr><td>X1A</td><td>Y1A</td></tr>
<tr><td>X1B</td><td>Y1B</td></tr>
<tr><td>X1C</td><td>Y1C</td><td>EEPROM 出错</td></tr>
<tr><td>X1D</td><td>Y1D</td><td>指令刷新</td></tr>
<tr><td>X1E</td><td>Y1E</td><td rowspan="2">无用</td></tr>
<tr><td>X1F</td><td>Y1F</td></tr>
</table>

3. 三菱 AS-i 网络通信

三菱 AS-i 网络通信也是两个过程。AS-i 模块与各个从站通信及 PLC CPU 与 AS-i 模块通信。其过程如图 3-25 所示。

QJ71AS92 与从站通信也是按 AS-i 规范轮询进行，其有关数据存放在它的缓冲区中。而

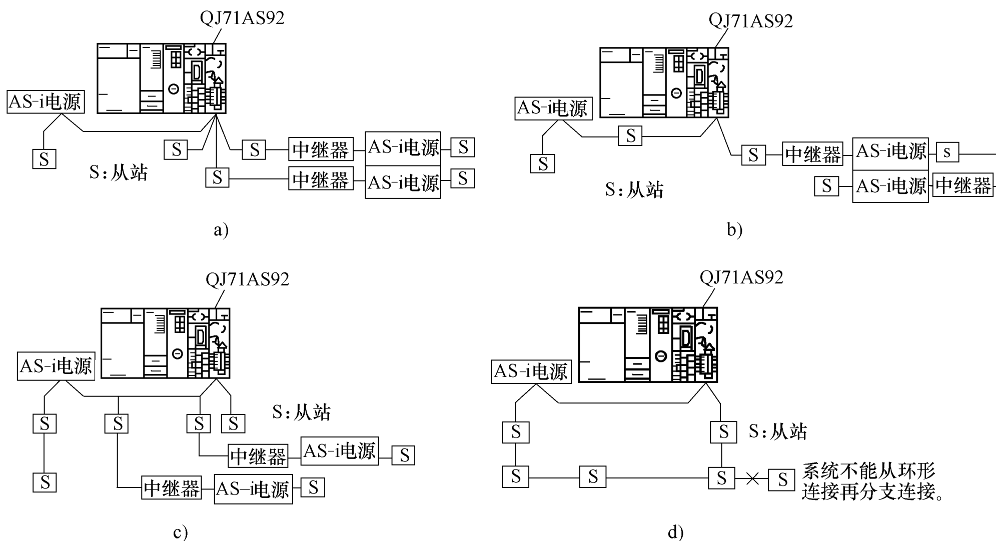


图 3-24　QJ71AS92 AS-i 系统连接方法示意

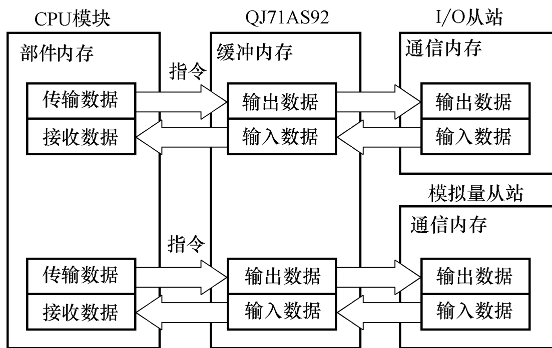


图 3-25　QJ71AS92 通信示意

PLC CPU 与模块通信，可用相应指令如同访问 PLC 其他内部器件一样，访问缓冲区；也可利用三菱提供的 AS-i 网络管理软件（GX Configurator-AS）对系统进行设置，然后直接访问。使用管理软件较简便，但软件要收费。

所使用的相关指令主要是传送、装载、输出等指令。但访问地址既要指出作为智能功能模块的 QJ71AS92 地址（在机架上的槽位），还要指明数据在从站在智能模块缓冲存储器内存区的地址。如地址 Un\G0，指的是槽号 n，缓冲区字地址为 0。

QJ71AS92 的缓冲内存区很大（其字地址从 000H ~ 7FFH）。既存放读写数据，还存放从站地址、工作命令、状态。

在缓冲区中最常用的是存放从站读写数据区。这些是：1A ~ 31A、1B ~ 31B 开关量输入区，有 1A ~ 31A、1B ~ 31B 开关量输出区，1B ~ 31B 模拟量输入区，1B ~ 31B 模拟量输出区。

从站 1A ~ 31A 开关量输入区存放缓冲区地址为 Un\G0 ~ Un\G7 之间。其中 Un\G0，指的是槽号 n，缓冲区字地址为 0，其存放的为从站 1A ~ 3A 数据，具体如图 3-26 所示。

而从站 4A ~ 31A 的数据则存放在缓冲区字地址 1H ~ 7H 之间（Un\G1 ~ Un\G7），见表 3-19 所示。

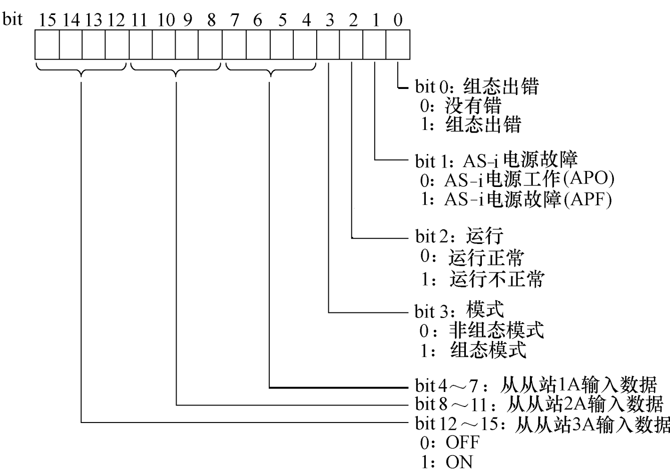


图 3-26　Un\G0 缓冲区存放从站 1A 到 3A 数据

表 3-19　从站 4A ~ 31A 数据在缓冲区中存放地址

bit	15 ~ 12	11 ~ 8	7 ~ 4	3 ~ 0
1H	7A	6A	5A	4A
2H	11A	10A	9A	8A
3H	15A	14A	13A	12A
4H	19A	18A	17A	16A
5H	23A	22A	21A	20A
6H	27A	26A	25A	24A
7H	31A	30A	29A	28A

从站 1B ~ 31B 开关量输入区存放缓冲区地址为 Un\G8 ~ Un\GFH 之间，见表 3-20 所示。

表 3-20　从站 1B 到 31B 输入数据在缓冲区中存放地址

bit	15 ~ 12	11 ~ 8	7 ~ 4	3 ~ 0
8H	3B	2B	1B	—
9H	7B	6B	5B	4B
AH	11B	10B	9B	8B
BH	15B	14B	13B	12B
CH	19B	18B	17B	16B
DH	23B	22B	21B	20B
EH	27B	26B	25B	24B
FH	31B	30B	29B	28B

—：未使用（0 fixed）
ON:1，OFF:0

从站 1A ~ 31A 开关量输出区存放缓冲区地址为 Un\G30H ~ Un\G37H 之间，见表 3-21 所示。

表 3-21　从站 1A ~ 31A 输出数据在缓冲区中存放地址

bit	15 ~ 12	11 ~ 8	7 ~ 4	3 ~ 0
30H	3A	2A	1A	(0000 fixed)
31H	7A	6A	5A	4A
32H	11A	10A	9A	8A
33H	15A	14A	13A	12A
34H	19A	18A	17A	16A
35H	23A	22A	21A	20A
36H	27A	26A	25A	24A
37H	31A	30A	29A	28A

从站 1B ~ 31B 开关量输出入区存放缓冲区地址为 Un\G38H ~ Un\G3FH 之间，见表3-22 所示。

表 3-22　从站 1B ~ 31B 输出数据在缓冲区中存放地址

bit	15 ~ 12	11 ~ 8	7 ~ 4	3 ~ 0
38H	3B	2B	1B	(0000 fixed)
39H	7B	6B	5B	4B
3AH	11B	10B	9B	8B
3BH	15B	14B	13B	12B
3CH	19B	18B	17B	16B
3DH	23B	22B	21B	20B
3EH	27B	26B	25B	24B
3FH	31B	30B	29B	28B

从站 1A ~ 31A 模拟量输入、输出数据存放的缓冲区地址为 E0H ~ 15FH，160H ~ 1DFH，见表 3-23 所示。

表 3-23　1A ~ 31A 模拟量输入、输出数据存放的缓冲区

地址		细节		地址		细节	
十六进制	十进制			十六进制	十进制		
E0 ~ E3	224 ~ 227	无效(固定为 0)		118 ~ 11B	280 ~ 283	从站地址 14	模拟量输出数据
E4 ~ E7	228 ~ 231	从站地址 1	模拟量输入数①	11C ~ 11F	284 ~ 287	从站地址 15	
E8 ~ EB	232 ~ 235	从站地址 2		120 ~ 123	288 ~ 291	从站地址 16	
EC ~ EF	236 ~ 239	从站地址 3		124 ~ 127	292 ~ 295	从站地址 17	
F0 ~ F3	240 ~ 243	从站地址 4		128 ~ 12B	296 ~ 299	从站地址 18	
F4 ~ F7	244 ~ 247	从站地址 5		12C ~ 12F	300 ~ 303	从站地址 19	
F8 ~ FB	248 ~ 251	从站地址 6		130 ~ 133	304 ~ 307	从站地址 20	
FC ~ FF	252 ~ 255	从站地址 7		134 ~ 137	308 ~ 311	从站地址 21	
100 ~ 103	256 ~ 259	从站地址 8		138 ~ 13B	312 ~ 315	从站地址 22	
104 ~ 107	260 ~ 263	从站地址 9		13C ~ 13F	316 ~ 319	从站地址 23	
108 ~ 10B	264 ~ 267	从站地址 10		140 ~ 143	320 ~ 323	从站地址 24	
10C ~ 10F	268 ~ 271	从站地址 11		144 ~ 147	324 ~ 327	从站地址 25	
110 ~ 113	272 ~ 275	从站地址 12		148 ~ 14B	328 ~ 331	从站地址 26	
114 ~ 117	276 ~ 279	从站地址 13		14C ~ 14F	332 ~ 335	从站地址 27	

（续）

地址		细节		地址		细节	
十六进制	十进制			十六进制	十进制		
150 ~ 153	336 ~ 339	从站地址 28	模拟量输出数据	198 ~ 19B	408 ~ 411	从站地址 14	模拟量输出数据
154 ~ 157	340 ~ 343	从站地址 29		19C ~ 19F	412 ~ 415	从站地址 15	
158 ~ 15B	344 ~ 347	从站地址 30		1A0 ~ 1A3	416 ~ 419	从站地址 16	
15B ~ 15F	348 ~ 351	从站地址 31		1A4 ~ 1A7	420 ~ 423	从站地址 17	
160 ~ 163	352 ~ 355	无效(固定为0)		1A8 ~ 1AB	424 ~ 427	从站地址 18	
164 ~ 167	356 ~ 359	从站地址 1		1AC ~ 1AF	428 ~ 431	从站地址 19	
168 ~ 16B	360 ~ 363	从站地址 2		1BD ~ 1B3	432 ~ 435	从站地址 20	
16C ~ 16F	364 ~ 367	从站地址 3		1B4 ~ 1B7	436 ~ 439	从站地址 21	
170 ~ 173	368 ~ 371	从站地址 4		1B8 ~ 1BB	440 ~ 443	从站地址 22	
174 ~ 177	372 ~ 375	从站地址 5		1BC ~ 1BF	444 ~ 447	从站地址 23	
178 ~ 17B	376 ~ 379	从站地址 6		1C0 ~ 1C3	448 ~ 451	从站地址 24	
17C ~ 17F	380 ~ 383	从站地址 7		1C4 ~ 1C7	452 ~ 455	从站地址 25	
180 ~ 183	384 ~ 387	从站地址 8		1C8 ~ 1CB	456 ~ 459	从站地址 26	
184 ~ 187	388 ~ 391	从站地址 9		1CC ~ 1CF	460 ~ 463	从站地址 27	
188 ~ 18B	392 ~ 395	从站地址 10		1D0 ~ 1D3	464 ~ 467	从站地址 28	
18C ~ 18F	396 ~ 399	从站地址 11		1D4 ~ 1D7	468 ~ 471	从站地址 29	
190 ~ 193	400 ~ 403	从站地址 12		1D8 ~ 1DB	472 ~ 475	从站地址 30	
194 ~ 197	404 ~ 407	从站地址 13		1DB ~ 1DF	476 ~ 479	从站地址 31	

① 当处非通信模式时，为1FFF（十六进制数）。

有关其他缓冲区存储数据细节建议读者使用时刻参阅三菱 AS-i 主站模块的说明书。

4. 三菱 AS-i 网络配置实例

（1）图 3-27 所示为三菱 AS-i 网络配置实例一

从图知，这里除了用到 QCPU 模块外，还有电源模块、QJ71AS92 模块、若干输入模块及输出模块。QJ71AS92 模块安装在机架的 0 槽位。AS-i 系统有 2 个从站（地址 4 的 4 点输出及地址 5 的 4 点输入）及 AS-i 电源。

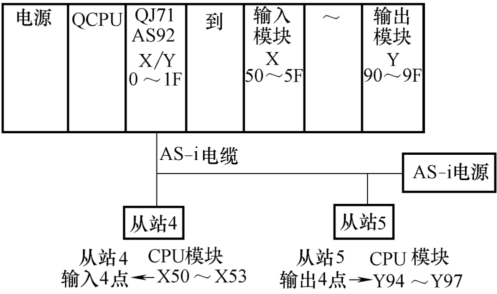


图 3-27 三菱 AS-i 网络配置实例

这个系统配置要求之一是，能把输入模块的 X0 ~ X3 能分别直接控制 AS-i 的从站 4 的 4 个输出点，而输出模块的 Y94 ~ Y97 能分别受 AS-i 的从站 5 的 4 个输入点直接控制。

实现此功能的相应梯形图程序如图 3-28 所示。

这里各个操作数的含义为

X0：模块就绪（当正常时，ON）；

X5：AS-I 电源故障（当正常时，OFF）；

X6：正常操作激活（当不正常时，OFF）；

X7：设置模式激活（当不是激活模式时，OFF）；

M104：当用于通信的地址 4 从站就绪时，ON；

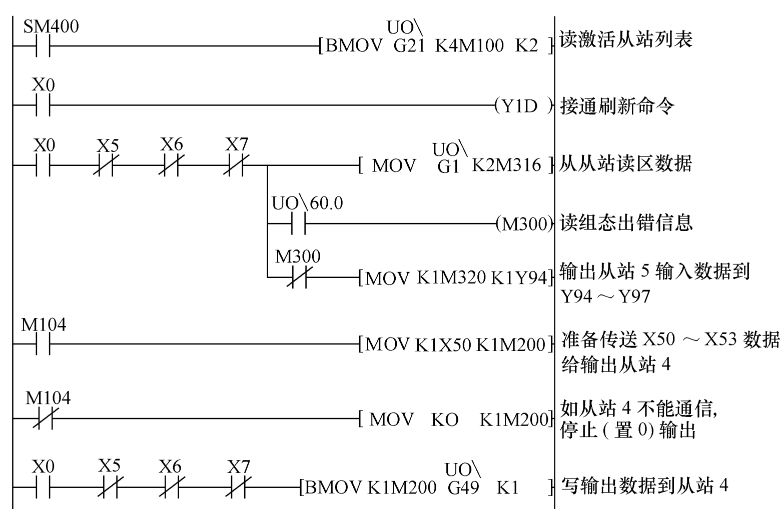


图 3-28　实现本例功能的梯形图程序

M200 ~ M203：到地址 4 从站输出数据；

M300：设置出错标志；

M320 ~ M323：从地址 5 从站输入数据。

（2）图 3-29 所示为三菱 AS-i 网络配置实例二

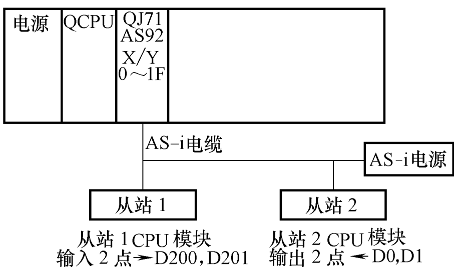


图 3-29　三菱 AS-i 网络配置实例

从图知，这里除了用到 QCPU 模块外，还有电源模块、QJ71AS92 模块、若干输入模块及输出模块。QJ71AS92 模块安装在机架的 0 槽位。AS-i 系统有 2 个从站（地址 1 的 2 路模拟量输入及地址 2 的 2 路模拟量输出）及 AS-i 电源。

这个系统配置要求之一是，能把 PLC 数据区 D0、D1 的现值能分别赋值给 AS-i 的从站 2 的 2 路模拟量输出，而 PLC 数据区 D200、D201 能分别读取 AS-i 的从站 1 的 2 路模拟量输入数据。

实现此功能的相应梯形图程序如图 3-30 所示。

这里各个操作数的含义为

X0：模块就绪（当正常时，ON）；

X5：AS-I 电源故障（当正常时，OFF）；

X6：正常操作激活（当不正常时，OFF）；

X7：设置模式激活（当不是激活模式时，OFF）；

M101：当用于通信的地址 1 从站就绪时，ON；

M102：当用于通信的地址 1 从站就绪时，ON；

D100：地址 1 模拟量从站数；

D101：地址 2 模拟量从站数；

D200，D201：地址 1 模拟量从站输入数据；

D400，D401：地址 2 模拟量从站输入数据。

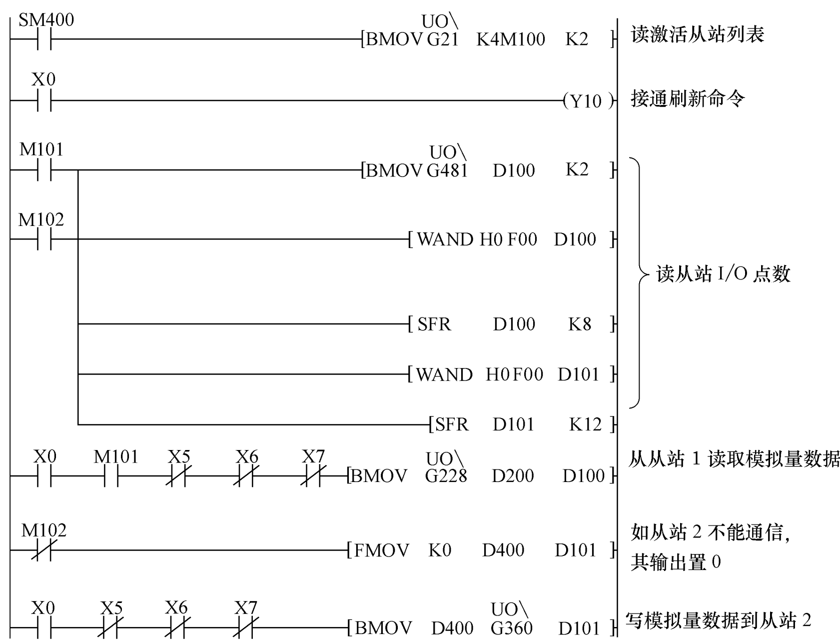


图 3-30　实现本例功能的梯形图程序

3.3　CC-Link/LT

关键词：主站、远程 I/O 站、RD、远程站、RAS、ONLINE 模式、Test 模式、Config 模式、缓冲存储器、点模式

CC-Link/LT 是将要在下一章介绍的 CC-Link 现场总线的简化。是专门为传感器、执行器和其他小型 I/O 的应用设计的。它与 CC-Link 的关系见表 3-24。

表 3-24　与 CC-Link 关系

	CC-Link	CC-Link/LT
开放性	完全开放的网络	
通信速度/(bit/s)	10M/5M/2.5M/625k/156k	2.5M/625K/156k
通信模式	循环传输、瞬时传输	循环传输
物理层	RS485	
I/O 站数量	64 站	
电缆	3 芯屏蔽电缆(3 芯通信)	4 芯电缆(2 芯信号,2 芯电源)
数据形式	位数据、字数据	位数据
点/站	32 点(远程 I/O)	2、8、16 点(远程 I/O)
通信模式	广播轮询加瞬时通信	广播轮询、间隔响应
传输格式	遵循 HDLC	遵循 HDLC + 特殊帧
错误校验	CRC	
编码方式	NRZI	
RAS 功能	网络测试和监控、回路自检测、子站脱离、自动上线恢复	

注 1. HDLC（High-Level Data Link Control），高级数据链路控制，是一个在同步网上传输数据、面向比特的数据链路层协议。

2. NRZI（No Return Zero-Inverse）非归零反相编码，信号从正电平到负电平的一次跃迁代表 1，没有电平变化代表 0。这里的跃迁有助于保持消息同步。

从表知，CC-Link/LT 为主从网。只能有一个主站，但可以有多达 64 个从站。网络由主站管理。网络通信由主站发起，从站响应，主站收到响应报文后，再访问下一站点。直到访问完最后站点又从头开始，周而复始，不断重复。

CC-Link/LT 主站主要是配置有主站模块的 PLC 或相关网桥，从站则是远程 I/O 站及字数据站。从实质上讲，CC-Link/LT 就是具有现场总线特征的 PLC 远程 I/O 网。以下将对它的组成、特点、拓扑结构、控制规格、组件及配置实例做简要介绍。

3.3.1　CC-Link/LT 简介

1. CC-Link/LK 网络组成

图 3-31 所示为 CC-Link/LK 网络组成示意。从图知，它有主站（主控模块）、远程 I/O 从站（模块）、24V 直流电源及电源适配器、电缆及终端电阻。

（1）主站

为配置有 CC-Link/LK 主站模块的 PLC 或既可连接 CC-Link 的主站又可连接 CC-Link/LK 从站的网桥。主站数据链接系统（Data Link System），除了与从站轮循传送信号，正常读写从站数据之外，还具有读取网络状态、控制网络工作的功能。网络要求有一个主站，也只能有一个主站。

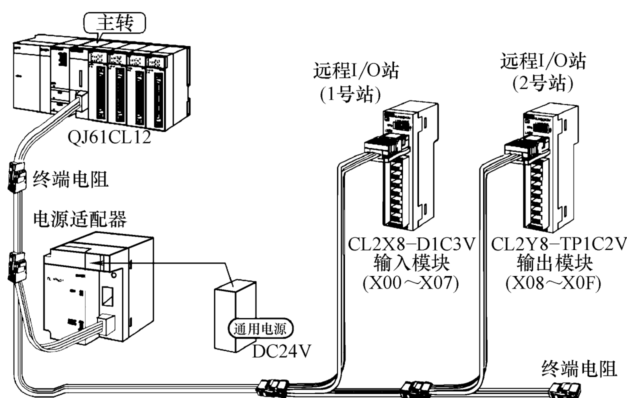


图 3-31　CC-Link/LK 网络组成

（2）从站

从站类型很多，仅能处理位的站称为远程 I/O 站。可读写字数据的站称为远程部件站（Remote Device，RD）站。运用模拟量与数字量转换模块还可读写模拟量。这两种站点统称远程站。一个网络最多可配置 64 个从站。但 I/O 点数多的从站可能要占据两个或多个站点号。这样，实际站点数有可能比 64 个要少。

要注意的是它与 CC-Link 从站是不兼容的。这从站不能接入 CC-Link。同样 CC-Link 的从站也不能接入它的主站。

（3）电源

为 24V 直流通用电源及其适配器。用以向从站提供工作电源。

（4）电缆

为四芯专用电缆。其中两根用以传输信号，两根用以提供从站工作电源。

（5）终端电阻及其他附件

终端电阻是必不可少的。分布在网络两端。一端在主站处，离主站不大于 200mm。另一端在最远处的从站外。此外，还有中继器、分支器，可根据需要配置，以扩展站点距离或建立分支结构。

2. CC-Link/LT 特点

（1）开放式网络技术

CC-Link/LT 利用和 CC-Link 相同的开放式网络技术。可从众多的供应商中灵活选择合适的设备，藉以提高系统构建的机动性。

（2）不需要参数设置

只有主站要求速度设置，从站不需要设置网络传输速度。

（3）编程简单

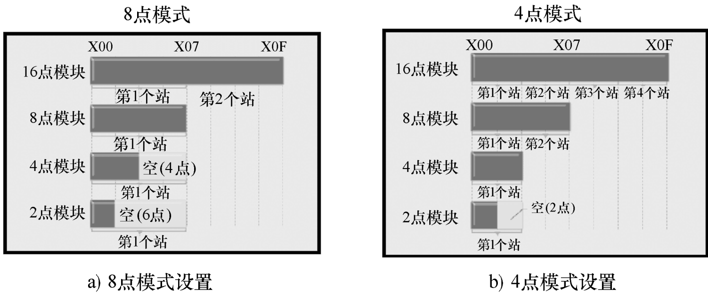
不需要特殊的网络指令或地址，CC-Link/LT 设备可以当作“本地 I/O”使用。

（4）丰富的 RAS 功能

这里说 CC-Link/LT 具备丰富的 RAS 功能，即指它具有网络诊断、内部回送诊断、从站脱离、自动恢复等功能。RAS 的含义是，可靠性（Reliability）、可用性（Availability）及可维护性（Serviceability）。

（5）可减少不用的 I/O 地址数量

通过点数模式设置，可将不用的 I/O 地址数减到最小。可从 4 点，8 点或 16 点模式中选择最合适的模式，从而获得对网络地址最有效的应用。图 3-32a、b 所示分别为 8 点模式与 4 点模式设置。



a) 8点模式设置　　b) 4点模式设置

图 3-32　8 点模式与 4 点模式设置

不过设定少的点模式，虽可以减少不用的 I/O 地址数量，但对 I/O 点数多的从站就要占据多个从站号。将减少网络可连接的总站数。

（6）简便有效的网络连接

使用 CC-Link“One-Touch”接插件，不需要特殊工具就能够进行快速、可靠的连接。这对于增加网络单元来说特别简便。此外，使用专用扁平电缆进行信号与电源传输，可消除配错线，并可减少更换模块的时间和减少接线费用。

（7）高速响应

CC-Link/LT 在 2.5Mbit/s 的网络通信速度时能够以 1.2ms 的极短时间快速更新所有的 I/O 点。根据应用中要求的电缆距离可以选择 3 种通信速度（2.5Mbit/s/625Kbit/s/156Kbit/s）。图 3-33 所示为为不同模式下的扫描时间。

（8）其他一些特点

此外有的还有其他一些特点。如在实施数据链接时可以停止和重新启动、电源开启后可检测从站占有点数和输入输出种类等信息，并存储到缓冲存储器中。

3. CC-Link/LT 拓扑结构

CC-Link/LT 为总线结构（干线），但可以建立 T 型分支（支线），如图 3-34 所示。有关规格见表 3-25。

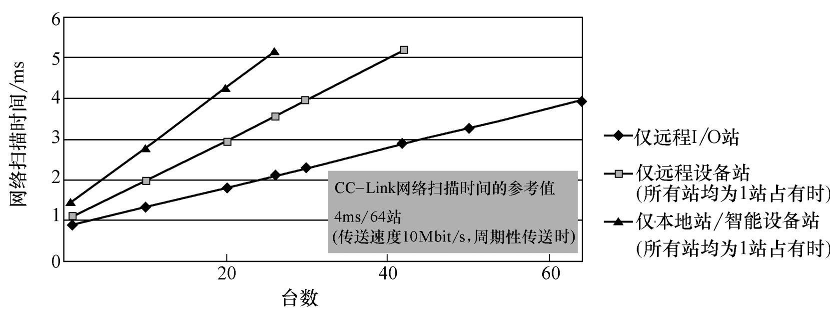


图 3-33 不同模式下的扫描时间

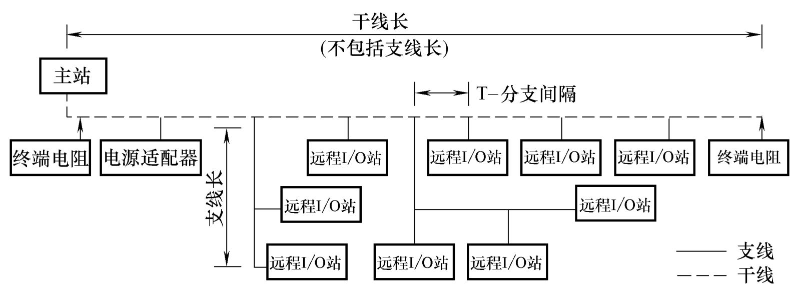


图 3-34 CC-Link/LT 拓扑结构

表 3-25 CC-Link/LT 接线规格

项 目	规 格			备 注
通信速度	2.5Mbit/s	625kbit/s	156kbit/s	—
站间距离	无限制			—
每一分支最多连接模块数	8			—
干线最大长度	35m	100m	500m	终端电阻间的电缆长不包括支线长
T-分支间隔	无限制			—
最大支线长	4m	16m	60m	每一分支电缆长度
支线总长	15m	50m	200m	支线的合计长

4. CC-Link/LT 控制规格

CC-Link/LT 控制规格见表 3-26。

表 3-26 CC-Link/LT 控制规格

项 目			4 点模式	8 点模式	16 点模式
最大链接点数,( )内为 I/O 都使用时			256 点(512 点)	512 点(1024 点)	1024 点(2048 点)
每个站连接点数,( )内为 I/O 都使用时			4 点(8 点)	8 点(16 点)	16 点(32 点)
链接扫描时间/ms	当连接32 个站	点数	128 点	256 点	512 点
		2.5M	0.7	0.8	1.0
		625kbit/s	2.2	2.7	3.8
		156kbit/s	8.0	10.0	14.1
	当连接64 个站	点数	256 点	512 点	1024 点
		2.5M	1.2	1.5	2.0
		625kbit/s	4.3	5.4	7.4
		156kbit/s	15.6	20.0	27.8

3.3.2 三菱 CC-Link/LT 组件

目前 CC-Link/LT 产品多为三菱公司生产，也以它比较齐全。三菱公司 CC-Link/LT 组件主要有：主站、从站及附件。

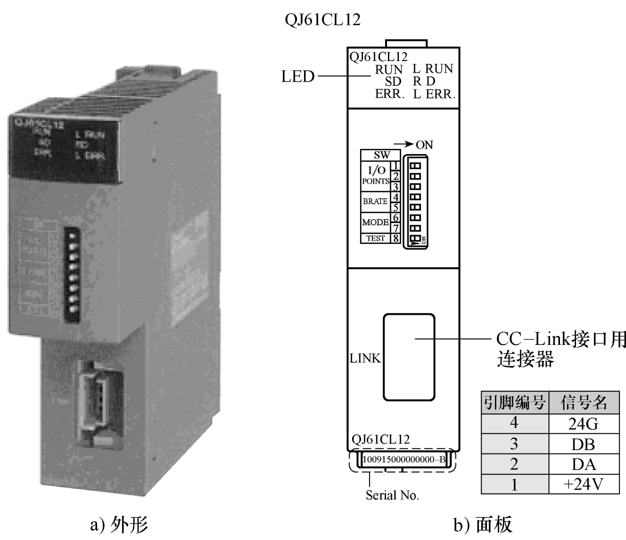
1. 主站模块

有 FX 机的 FX2N -64CL-M、FX3UC 机的 FX3UC-32MT-LT 及 Q 系列机的 QJ61CL12 模块。此外还有与 CC-Link 连接的 AJ65SBT-CLB 桥接模块。

(1) QJ61CL12

其外形与面板外观如图 3-35 所示。

1) 面板。其面板上有指示灯、设定开关及网络接口用连接器。其指示灯（LED）含义见表 3-27。其设定开关可用以设定输入输出点数、传输速度、点数模式及工作模式。具体见表 3-28。



a) 外形　　b) 面板

图 3-35　QJ61CL12 外形与面板

表 3-27　QJ61CL12 指示灯（LED）含义

LED 名称	LED 内容
RUN	亮灯:模块工作正常
ERR.	亮灯:开关设置异常
	闪烁:工作中切换开关
L RUN	亮灯:正在执行数据链接
L ERR.	亮灯:数据链接异常站(检测)、有控制范围外的站
	闪烁:数据链接异常站(全站)
SD	亮灯:正在发送数据
RD	亮灯:正在接收数据

表 3-28　输入输出点数、传输速度、点数模式及工作模式设定

输入输出占用点数		16 点	32 点	48 点	64 点	128 点	256 点	512 点	1024 点
1	I/O POINTS	OFF	OFF	OFF	ON	OFF	OFF	OFF	ON
2		OFF	ON	ON	OFF	OFF	OFF	ON	ON
3		OFF	ON	OFF	ON	ON	ON	ON	ON
传送速度设置		156kbit/s		625kbit/s		2.5Mbit/s		禁止设置①	
4	B RATE	OFF		OFF		ON		OFF	
5		OFF		ON		ON		ON	
点数模式设置		8 点		4 点		16 点		禁止设置①	
6	MODE	OFF		OFF		ON		OFF	
7		OFF		ON		ON		ON	
测试模式		OFF:在线(通常动作)							
8	TEST	ON:测试模式(折返测试)							

① 设置为禁止设置时 ERR. LED 亮灯。

2）该模块可作为智能模块安装于 Q 系列机架上。可与其连接的 CPU 见表 3-29。

表 3-29　可连接的 CPU

可连接的 CPU 型号名		可安装块数
QCPU 高性能型	Q02CPU, Q02HCPU, Q06HCPU, Q12HCPU, Q25HCPU	最多 64 块①
QCPU 基本型	Q00JCPU②, Q00CPU, Q01CPU	
过程 CPU	Q12PHCPU, Q25PHCPU	
NET/H 远程站	QJ72LP25-25, QJ72LP25G(E), QJ72BR15	
个人电脑 CPU③	PPC-CPU686(MS)-64, PPC-CPU686(MS)-128	

① 因主控模块的输入输出占用点数设置不同可安装的块数也不同。

② Q00JCPU 的 I/O 点数最大为 256 点，所以 I/O 点数的可使用数不能超过 256 点的范围。（如果设置的输入输出占用点数超过 256 点，则在 Q00JCPU-侧检测到出错，CPU 不工作）。

③ 个人电脑 CPU 是康泰克株式会社制造的。

QJ61CL12 可以安装在基板的任意 I/O 插槽中。然而根据它与其他安装模块的组合情况及所用的模块数可能出现电源电压不足现象，因此在安装模块时一定要考虑电源容量问题。

3）主站动作（工作）模式。有在线（ONLINE）模式及测试（TEST）模式。

① ONLINE 模式是进行 CC-Link/LT 系统的数据链接。一般使用时，请选择此模式。

② TEST 模式（自我折返测试）。此测试不需连接远程站（请设定 DIP 开关，接通 PLC 的电源）。开始测试，确认状态显示 LED。自我折返测试将在数秒中内完了。状态显示 LED 为 L RUN 灯亮时正常、L ERR. 灯亮时为异常。

4）PLC CPU 的输入输出信号。X 分配为远程输入。Y 分配为远程输出。并根据设定的点数模式不同，输入输出信号的分配有所不同。表 3-30 所示为 4 点模式设置时的输入输出信号一览表。而 8 点、16 点模式则各站所占的 X、Y 点号以 16 进制的规则类推。有了这个 I/O 分配，直接对这个地址读写，即可实现远程通信。

表 3-30　4 点模式设置时的输入输出信号一览表

输入编号	远程输入(X)															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
XnF ~ Xn0	4 号站				3 号站				2 号站				1 号站			
≀	≀															
X(n+F)F ~ X(n+F)0	64 号站				63 号站				62 号站				61 号站			
输出编号	远程输出(Y)															
	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
YnF ~ Yn0	4 号站				3 号站				2 号站				1 号站			
≀	≀															
Y(n+F)F ~ Y(n+F)0	64 号站				63 号站				62 号站				61 号站			

注：这里的 n 是 QJ61CL12 的起始输入输出编号。例 QJ61CL12 的起始输入输出编号为 X30/Y30，则 Xn0 ~ XnF 为 X30 ~ X3F，Yn0 ~ YnF 为 Y30 ~ Y3F。

要指出的是，选用小的点模式可节省内存，还可减少扫描时间，但由于从站数不能超过 64，所以将减少可控制的 I/O 点数。所以，这两者设置要在确保可控制点数的前提下，尽量选用小的点数模式。

5）缓冲存储器。主站模块的缓冲存储器存储网络的控制命令、状态信息及与各从站通信数据。PLC CPU 可用编程软件 GX Developer 或者顺控程序对其读写。其与各从站通信数据则是通过 I/O 刷新与上述输入输出信号（X/Y）交换。缓冲器存储器的地址、项目及是否可读写见表 3-31。

表 3-31　缓冲存储器一览表

地址		项　目	可否读写
十进制	十六进制		
0 ~ 3	0H ~ 3H	远程站连接信息	读出专用
4 ~ 7	4H ~ 7H	异常站信息	读出专用
8 ~ 11	8H ~ BH	远程输入输出信息	读出专用
12 ~ 15	CH ~ FH	禁止使用①	—
16	10H	出错详细信息	可以读出/写入
17	11H	外部开关信息	读出专用
18	12H	运行状态信息	读出专用
19	13H	数据链接的停止/再起动指示	写入专用
20	14H	数据链接的最终站信息	读出专用
21 ~ 31	15H ~ 1FH	禁止使用①	—
32	20H	远程站详细信息(1 号站)	读出专用
≀	≀	≀	
95	5FH	远程站详细信息(64 号站)	
96 ~	60H ~	禁止使用①	—

① 禁止使用的区内不能进行写入否则可能出错。

其中远程站连接信息（缓冲存储器地址 0-3：Un\G0-3）、异常站信息（缓冲存储器地址 4-7：Un\G4-7）、运行状态信息（缓冲存储器地址 18：Un\G18）及数据链接的停止/再起动指示（缓冲存储器地址 19：Un\G19）分别见见表 3-32 ~ 表 3-35。其他详细信息科参阅该模块说明书。

表 3-32　远程站连接信息

地址(十进数)	b15	b14	b13	~	b2	b1	b0
0	16 号站	15	14 号站	~	3 号站	2 号站	1 号站
1	32 号站	31 号站	30 号站	~	19 号站	18 号站	17 号站
2	48 号站	47 号站	46 号站	~	35 号站	34 号站	33 号站
3	64 号站	63 号站	62 号站	~	51 号站	50 号站	49 号站

注：0 无远程站连接；1 有远程站连接。

表 3-33　远程站异常连接信息

地址(十进数)	b15	b14	b13	~	b2	b1	b0
4	16 号站	15 号站	14 号站	~	3 号站	2 号站	1 号站
5	32 号站	31 号站	30 号站	~	19 号站	18 号站	17 号站
6	48 号站	47 号站	46 号站	~	35 号站	34 号站	33 号站
7	64 号站	63 号站	62 号站	~	51 号站	50 号站	49 号站

注：0 工作正常；1 工作异常。

表 3-34　运行状态信息

位	名　称	内　容
b0	数据链接状态	0:数据链接停止中 1:正在进行数据链接
b1	初始通信状态	0:初始通信未结果 1:初始通信结束
b15 ~ b2	空	—

表 3-35　数据链接的停止/再起动指示

位	名　称	内　容
b0	数据链接停止	0:无数据链接停止请求 1:有数据链接停止请求
b14 ~ b1	空	—
b15	数据链接再起动	0:无数据链接再起动请求 1:有数据链接再起动请求

注：控制数据链接停止和再起动同时请求时，以数据链接停止为优先。

（2）FX2N -64CL-M

其外形及面板外观如图 3-36 所示。

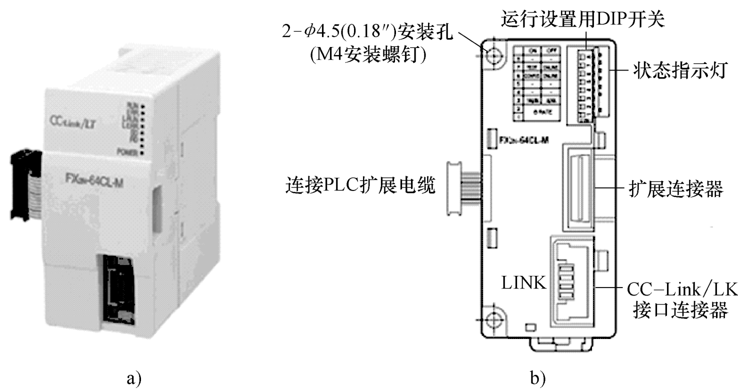


图 3-36　FX2N-64CL-M 外形与面板外观

1）面板。其面板上有指示灯、设定开关及网络接口用连接器。其指示灯（LED）含义见表 3-36。其 DIP 开关可用以设定输入输出点数、传输速度、点数模式及工作模式。具体见表 3-37。

要说明的是，DIP 开关出厂是默认为全部 OFF。当同时选 CONFIG 和 TEST 模式时为 TEST 模式。在上电后改变设定无效（只有再上电后才有效）。

2）与 CPU 连接。该模块可作为智能扩展模块与于 FX 系列的 CPU 机架相连。可与其连接的 CPU 模块及其他特性见表 3-38。

对 FX3UC 这个三菱公司最新的小型 PC，除了可安装该模块，还有内置 CC-Link/LT 主站的 CPU 模块（FX3UC -32MT-LT）。此外，还可连接上述 CC-Link/LT 主站模块，如表所示可最大连接 7 台这样特殊扩展模块。但是，输入输出点数不能超过最大 256 点。

表 3-36　QJ61CL12 指示灯（LED）含义

Power	在线模式/配置模式/测试模式 亮:电源供电 灭:电源不供电
RUN	在线模式/配置模式/测试模式 亮:模块工作正常 灭:模块工作不正常
ERR	在线模式: 亮:通信速率设定错 EERAM 读出错 闪烁:通信供电不正常 DIP 开关改变 灭:模块工作正常 配置模式: 亮:通信速率设定错 EERAM 写出错 闪烁:通信供电不正常 DIP 开关改变 灭:模块工作正常 测试模式: 亮:通信速率设定错 EERAM 读出错 闪烁:通信供电不正常 DIP 开关改变 灭:模块工作正常
L RUN	在线模式/配置模式/测试模式 亮:进行数据链接 灭:数据链接停止
L ERR	在线模式: 亮:所用站数不符 　所控制站超出范围 闪烁:若干站工作不正常 灭:数据链接正常 配置模式: 亮:所用站数不符 　所控制站超出范围 闪烁:所有站工作不正常 灭:数据链接正常 测试模式: 亮:回路自测不正常 闪烁:回路自测正常
SD	在线模式/配置模式/测试模式 正发生数据
RD	在线模式/配置模式/测试模式 正接收数据

表 3-37　输入输出点数、传输速度、点数模式及工作模式的 DIP 开关设定

<table>
<tr><td>1</td><td rowspan="2">波特率</td><td rowspan="2">通信速度设置<table><tr><td>通信速率</td><td>SW1</td><td>SW2</td></tr><tr><td>156kbit/s</td><td>OFF</td><td>OFF</td></tr><tr><td>625kbit/s</td><td>ON</td><td>OFF</td></tr><tr><td>2. 5Mbit/s</td><td>OFF</td><td>ON</td></tr><tr><td>设置禁止</td><td>ON</td><td>ON</td></tr></table></td></tr>
<tr><td>2</td></tr>
<tr><td>3</td><td>16 点/4 点</td><td>点模式设置(选择每站 I/O 点数)
OFF:4 点模式(每站 4 点入,4 点出)
ON:16 点模式(每站 16 点入,16 点出)</td></tr>
<tr><td>4</td><td>—</td><td>设置禁止(确认当运行时处 OFF)</td></tr>
<tr><td>5</td><td>—</td><td>设置禁止(确认当运行时处 OFF)</td></tr>
<tr><td>6</td><td>组态/在线</td><td>组态模式
OFF:在线模式(正常操作)
ON:组态模式(被连接站信息存贮于 EEPROM 中)</td></tr>
<tr><td>7</td><td>测试/在线</td><td>测试模式
OFF:在线模式(正常操作)
ON:测试模式(字回馈测试)</td></tr>
<tr><td>8</td><td>—</td><td>设置禁止(确认当运行时处 OFF)</td></tr>
</table>

表 3-38　可连接的 CPU 及其他特性

项　　目	特　　性
可使用的 PLC	FX1N、FX2N、FX2NC、FX3U、FX3UC 系列 PLC (当连接 FX2NC 系列 PLC 时要求用 FX2NC-CNV-IF) (当连接 FX3UC 系列 PLC 时要求用 FX2NC-CNV-IF 或 FX3UC-1PF-5V)

（续）

项　目				特　性	
可连接模块数				FX1N系列PLC最多4个,FX2N系列PLC最多8个 FX2NC系列PLC最多3个,FX3U系列PLC最多8个 FX3UC系列PLC最多8个	
可选用的点模式				4点和16点模式,可用DIP开关选定	
控制规格				4点模式	16点模式
控制规格	最多连接点数			连接到FX1N系列PLC:128点 连接到FX2N、FX2NC、FX3U、FX3UC系列PLC:256点(含每个PLC的I/O点数)	
控制规格	每站连接点数 ( )表示当使用混合远程模式的点数			4点(8点)	16点(32点)
控制规格	链接扫描时间	32站	点	128点	256点
控制规格	链接扫描时间	32站	2.5Mbit/s	0.7ms	1.0ms
控制规格	链接扫描时间	32站	625kbit/s	2.2ms	3.8ms
控制规格	链接扫描时间	32站	156kbit/s	8.0ms	14.1ms
控制规格	链接扫描时间	64站	点	256点	256点
控制规格	链接扫描时间	64站	2.5Mbit/s	1.2ms	2.0ms
控制规格	链接扫描时间	64站	625kbit/s	4.3ms	7.4ms
控制规格	链接扫描时间	64站	156kbit/s	15.6ms	27.8ms
通信规格	通信速率			2.5Mbit/s,625kbit/s,156kbit/s	
通信规格	协议			BITR方法(广播加内部定时)	
通信规格	网络拓扑			T分支	
通信规格	出错控制方法			CRC	
通信规格	连接站数			最多64	
通信规格	远程站数			1~64	
通信规格	主站连接位置			连接在主干线端点	
通信规格	RAS功能			通信出错检测,系统自动复位,从站断线检测与内部回路诊断	
通信规格	连接电缆			专用扁平电缆(0.75mm^2*4),VCTF电缆(0.75mm^2*4),高柔软电缆(0.75mm^2*4)	
内部电流消耗				190mA(PLC通过扩展连接器提供)	
DC 24直流电源			电压	DC 20.4~28.8V	通过连接器电源适配器或专用电源供电
DC 24直流电源			消耗电流	35mA	通过连接器电源适配器或专用电源供电
DC 24直流电源			初始电流	35mA	通过连接器电源适配器或专用电源供电
重量				0.15kg	

注：1. 当连接FX1N系列PLC时，最多可安装2个FX2N-64CL-M模块；
2. FX2N-64CL-M要消耗190mA电流（自DC 5V电源）；
3. 当连接FX3UC-32MT-LT PLC时，最多可安装两个FX2N-64CL-M模块。

3）主站动作（工作）模式。有在线（ONLINE）模式、配置（CONFIG）模式及测试（TEST）模式。

① ONLINE模式是进行CC-Link/LT系统的数据链接。一般使用时，请选择此模式。

② CONFIG模式。CC-Link/LT的系统结构完成后，可利用CONFIG模式进行自动的输入输出编号分配。所收集连接的远程站的信息（输入输出的种类和点数），将暂存至缓冲存

储器［BFM #32（20h）~#95（5Fh）］和内置存储器（EEPROM）上。若将来有扩展远程站的预定时，也可预先将输入输出编号做空号暂留。

③ TEST 模式（自我折返测试）。此测试不需连接远程站（请设定 DIP 开关，接通 PLC 的电源）。开始测试，确认状态显示 LED。自我折返测试将在数秒中内完了。状态显示 LED 为 L RUN 灯亮时正常、L ERR. 灯亮时为异常。

4）输入输出编号的分配。在配置模式 FX2N-64CL-M 会自动为从站指定在 PLC 上的 X（输入）、Y（输出）地址。地址以八进制进位。开始地址接续在 PLC 已占用 I/O 地址之后。由于它具有配置模式，为这个地址分配提供了很大方便。至于点模式及可控制 I/O 点数处理与 Q 系列模块相同。

5）缓冲存储器。与 Q 系列模块相比基本相同，但增大了，也增加内容。有的与增加配置模式有关。还有就是对 RD 的访问。如它在高地址处，也可用 FROM、TO 这里访问，其数据也可为 PLC 使用。但如果这高地址不是 RD 站，则访问被拒绝。缓冲器存储器的地址、项目及是否可读写见表 3-39。

表 3-39　缓冲存储器一览表

缓冲区地址		名　称	说　明	R(读) W(写)
十进制	十六进制			
0~3	0H~3H	远程站连接信息	存储每一远程站连接信息 (当远程站连接时相应位 ON)	R
4~7	4H~7H	链接出错站信息	存储每一远程站连接状态	R
8~11	8~BH	远程 I/O 出错信息	存储 I 每从站/O 出错信息	R
12~15	CH~FH	禁止使用		…
16~19	10H~13H	保留站信息	存储保留站设置状态	R
20	14H	要求输入块数	存储输入快数(按 8 点为单位计)	R
21	15H	要求输出块数	存储输出快数(按 8 点为单位计)	R
22	16H	数据链接终站信息	存储可使用的终站号	R
23~25	17H~19H	禁止使用		…
26	1AH	扩展开关信息	存储 DIP 开关设置状态	R
27	1BH	命令	给 FX2N-64CL-M 指令,已停止与再起始数据链接 并存储此信息到 EEPROM 中	R/W
28	1CH	状态信息	存储诸如 RUN 及链接等状态信息	R
29	1DH	详细出错信息	存储被 FX2N-64CL-M 检测到的详细出错信息	R
30	1EH	模块编码	K7120	R
31	1FH	禁止使用		…
32	20H	详细远程站信息(站 1)	存储站 1 信息(I/O 类型及点数),在组态模式此信息可编辑	R/W
· · ·	· · ·	· · ·	· · ·	· · ·
95	5FH	详细远程站信息(站 64)	存储站 64 信息(I/O 类型及点数),在组态模式此信息可编辑	R/W
96~143	60H~8FH	禁止使用	…	…

（续）

缓冲区地址		名　称	说　明	R(读) W(写)
十进制	十六进制			
144	90H	远程输入区(站 49)	从远程站访问输入数据	R
145	91H	远程输入区(站 50)		
· · ·	· · ·	· · ·	· · ·	· · ·
158	5EH	远程输入区(站 63)	从远程站访问输入数据	R
159	5FH	远程输入区(站 64)		
160 ~ 207	A0H ~ CFH	禁止使用	…	…
208	D0H	远程输出区(站 49)	从远程站访问输出数据	R/W
209	D1H	远程输出区(站 50)		
· · ·	· · ·	· · ·		· · ·
222	DEH	远程输出区(站 63)	从远程站访问输出数据	R/W
223	DFH	远程输出区(站 64)		

（3） 网桥模块

如 AJ65SBT-CLB 可用以把 CC-Link/LT 从站接入 CC-Link 网络。图 3-37 所示为该模块用以实现上述连接的情况。

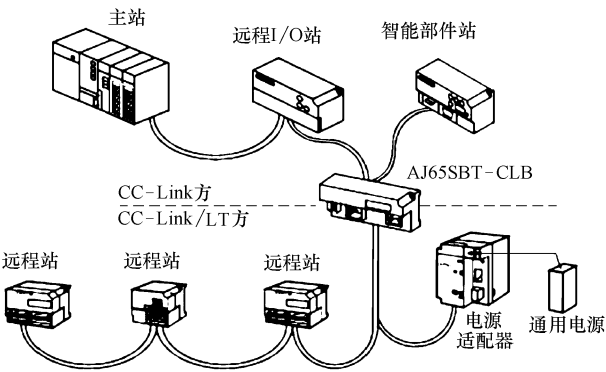


图 3-37　CC-Link/LT 从站接入 CC-Link 网络示意

2. 从站模块

从站模块较多。按结构分有 4 种类型，即端子座型、传感器连接器型、MIL 连接器型及电缆型。可用于不同的现场设备的连接。图 3-38 所示为这 4 种类型从站的外观与特点。

● 端子座型

适合于压接端子的连接。
常用的连接方式。

● 传感器连接器型

便于连接传感器等。

● MIL连接器型

便于配线作业，装置在附近时便于使用。

● 电缆型

可直接给传感器等配线。

图 3-38　4 种类型从站的外观及特点

其主要产品机器性能见表 3-40。

表 3-40 从站主要产品及其性能

类　型	型　号	性　能
端子座型	AJ65SBT-CLB	CC-Link ~ CC-Link/LT 桥模块
	CL1X4-D1B2	输入 4 点:DC 24V(正公共端/负公共端型共用)
	CL1Y4-T1B2	输出 4 点:DC 24V(漏型)0.1A 晶体管输出
	CL1Y4-R1B2	输出 4 点:DC 30V　AC250V 以下　2A 继电器输出
	CL2X8-D1B2	输入 8 点:DC 24V(正公共端/负公共端型共用)
	CL2Y8-TP1B2	输出 8 点:DC 24V(漏型)0.1A 晶体管输出(带输出保护功能)
	CL1XY8-DT1B2	输入 4 点:DC 24V(正公共端/负公共端型共用)
	CL1XY8-DR1B2	输出 4 点;DC 24V(漏型)0.1A 晶体管输出
传感器连接器型	CL2X8-D1C3V	输入 4 点:DC 24V(正公共端/负公共端型共用)
	CL2Y8-TP1C2V	输出 4 点:DC 30V　AC250V 以下　2A 继电器输出
MIL 连接器型	CL2X16-D1M1V	输入 8 点:DC 24V(正公共端型)
	CL2Y16-TP1M1V	输出 8 点:DC 24V(漏型)0.1A 晶体管输出(带输出保护功能)
电缆型	CL1X2-D1D3S	输入 16 点:DC 24V(正公共端型)0.1A 晶体管输出(带输出保护功能)
	CL1Y2-T1D2S	输入 2 点:DC 24V(正公共端型)　输出 2 点:DC 24V(漏型)0.1A 晶体管输出
	CL1XY2-DT1DSS	输入 1 点:DC 24V(正公共端型)

此外，还有数字量到模拟量相互转换的模块，可用于模拟量的输入（CL2AD4-B）或输出（CL2DA2-B）。每个模块有 4 个模拟量通道，但要占用 4 个站号（对 16 点模式）。而模拟量与数字量对应关系可按表 3-41 确定。转换精度与环境条件有关。

表 3-41 模拟量与数字量对应关系

	输入范围	数字量
电压/V	-10 ~ +10	-4000 ~ +4000
	0 ~ +10	0 ~ +4000
	0 ~ +5	
	1 ~ +5	
电流/mA	0 ~ 20	0 ~ +4000
	4 ~ 20	

3. 电源模块

CC-Link 必须另加网络电源，以供主站及从站各模块使用。所选的电源模块的容量要满足网络各站点消耗电流的要求。而各个站点模块电流消耗见有关说明书。如果总电流大过 5A，还必须再另增加电源。网络线路压降也不能超过 3.6V，要确保各个站点的电压不低于 20V。否则也要在网络的适当位置另增加电源。压降与总线的铺设距离有关。其计算有简易法及精确法。具体见关电源模块的说明书。

3.3.3 三菱 CC-Link/LT 配置过程及实例

1. Q 系列 PLC CC-Link/LT 配置步骤及实例

(1) 配置步骤。大体为

1）把 QJ62CL12 模块安装在基板上。在控制板及机器上，安装 PLC、远程模块及专用电源或电源适配器。

2）通过电缆连接 QJ62CL12 模块、远程模块及专用电源或电源适配器。并在主干线终端接终端电阻。这里的安装细节很多，注意点也很多。务必要按有关说明书要求处理。

3）在 QJ62CL12 模块面板上，用 IP 开关设置点模式、输入输出占有点数及传输速率。设置各从站站号。

对使用 QJ62CL12 模块，点数模式分为 4 点模式、8 点模式、16 点模式 3 种。即使是设置为相同的输入输出占用点数，因点数模式的设置不同，则能够控制的远程站的站数也不同。输入输出占用点数与点数模式设置的关系见表 3-42 所示。

表 3-42　点数模式与连接站数关系

输入输出占用点数的设置		16 点	32 点	48 点	64 点	128 点	256 点	512 点	1024 点
点数模式的设置	4 点模式	4 个站	8 个站	12 个站	16 个站	32 个站	64 个站	64 个站	64 个站
	8 点模式	2 个站	4 个站	6 个站	8 个站	16 个站	32 个站	64 个站	64 个站
	16 点模	1 个站	2 个站	3 个站	4 个站	8 个站	16 个站	32 个站	64 个站

如果所设置的输入输出占用点数比 4 点模式和 8 点模式的最多链接点数还要大，则超过 4 点模式和 8 点模式的最多链接点数的部分的输入输出部分的点数不能使用。例点数模式为 4 点模式，输入输出占有点数设置为 1024 点时，虽然 QJ61CL12 占用 1024 点的 PLC CPU 的输入输出点数，但是实际上可以使用的链接点数只有 256 点。因 4 点模式的最多链接点数为 256 点（最多智能有 64 个从站），剩余的 768 点不能使用。再就是，点数模式的设置不同，即使是相同的远程模块其占用的站数也不同。例如 16 点模块时，如果设置为 4 点模式、8 点模式 、16 点模式，则分别占用 4 个站号、2 个站号及 1 个站号。至于选择多少点数的模式为好，则要根据所使用的远程模块的点数不同而不同。但作为基本的考虑方法是，如果将点数模式设置为站数最多的远程模块的点数，就能减少无用的空点数。

传输速率与拓扑结构、站点距离及环境有关。在确保传输可靠的基础上，尽量设高些。远程站号不能重复。如果重复将出错，可能无法工作或产生误动作。

4）最终站号设置。是为了设置所连接的远程站的最终站。之后的站点物理上虽与主站相连，但不做数据链接，不交换数据。最终站编号设置并不是必须进行的。但是在希望链接扫描时间最佳化时，可进行设置。具体设置要用到 GX Developer 编程软件，在添加的模块特性项选定。如 16 点模式，输入输出点数设置为 128 点，所连接的远程站的最终站为 5 站时，通过把最终站设置为 5，就能使链接扫描时间最佳化。

5）在接通电源前要确认模块安装状态，确认向电源适配器输入电压（DC 24V），确认 CPU 的 RUN/STOP 开关处 STOP 位置，确认 CPU 的 RESET 开关处于中央位置。确保远程站的站号没有重复。

6）接通电源。察看指示灯，确认 QJ62CL12 模块运行状态。如数据链接正常时，L RUN 灯点亮，如链接异常，L ERR 灯点亮或闪烁。设置异常时，ERR 等点亮。

7）确认各模块的连接状态。可用远程连接性信息确认，或用通过 CC-Link/LK 诊断确认。

8）编写程序、下载给 PLC，网络电源接通，PLC 出运行状态，系统即可工作。

（2）配置实例

如图 3-39 所示。有 4 输入点远程站 1 个，8 输入点远程站 1 个，4 输出点远程站 1 个，2 输出点远程站 1 个、16 输入点远程站 1 个、4 输入点远程站 1 个及 4 输出点远程站 1 个。

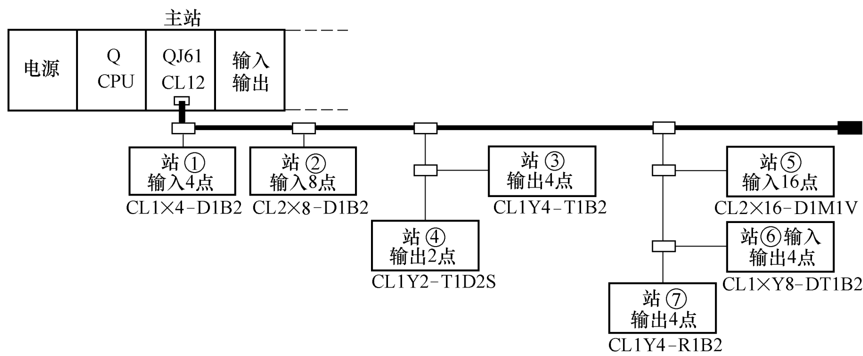


图 3-39 q 系列机 CC-Link/LT 配置实例

系统配置主要的是做好点数模式设置。如果按照选择数量最多的远程 I/O 模块的占有点数作为点数模式的原则设置，则本例点数模式设置选择 4 点模式，产生的空点数最少。图 3-40所示为点数模式设置时空点数的情况。

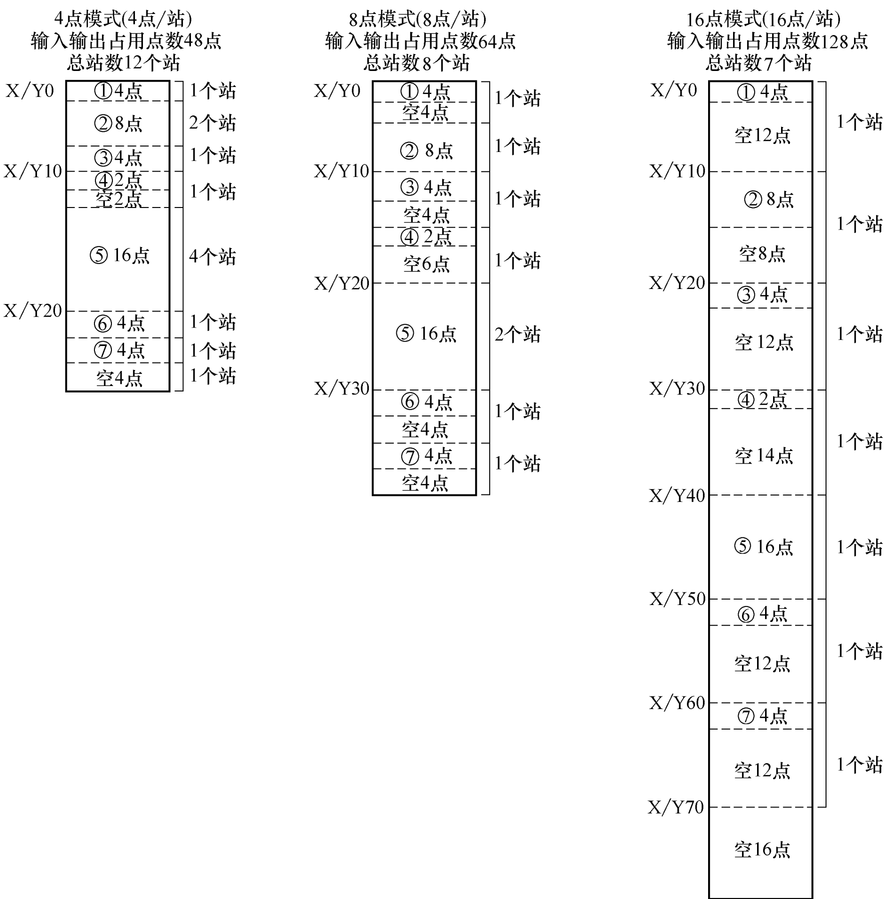


图 3-40 不同点数模式设置时空点数情况

只是要注意点数模式设置为 4 点模式或 8 点模式时，根据所使用的远程站的不同，可能有占用多个站号的站点。为此，要注意有一些站点多占站号而造成重复站号。此外，系统在运行中，如果要变更设置，则必须让系统断电，再上电后，所改变的设置才有效。

因此，本例点数模式设置为 4 点模式。传送速度设置 2.5Mbit/s。其输入（X）、输出（Y）分配见以上介绍的表 3-42 的 4 点模式设置时的输入输出与站号对应关系表。有了此表，加上模块缓冲区的其他数据，即可按要求编程实现对远程 I/O 的控制或数据采集了。

2. FX 系列 PLC CC-Link/LT 配置步骤及实例

（1）配置步骤。大体为

1）在控制板及机器上，安装 FX2N-64CL-M 模块、远程模块及专用电源或电源适配器。

2）通过电缆连接 FX2N-64CL-M、远程模块及专用电源或电源适配器。并在主干线终端接终端电阻。从站的连接顺序与站号无关，在 FX2N-64CL-M 模块如再接其他特殊模块，将不工作，等等。但是这里的安装细节很多，注意点也很多。务必要按有关说明书要求处理。

3）用模块面板上的 DIP 开关，设置 FX2N-64CL-M 与远程站的传输速率、点模式、站号等。并置 FX2N-64CL-M 处配置（CONFIG）模式。

4）在接通电源前检查以下各项：确认 FX2N-64CL-M、远程站及专用电源或电源适配器的安装状态；确认加给专用电源或电源适配器的电压；确认 RUN/STOP 开关处 STOP 状态；确认远程从站没有相同的站号。

5）先接通专用电源或电源适配器电源，后接通 PLC 电源，执行配置（CONFIG）模式。这时，无须参数设置与执行程序，FX2N-64CL-M 模块即可为远程站自动指定 I/O 地址。

要注意这里的 I/O 编号与点数模式无关。但不同模式远程站号不同。16 点模式比 4 点模式可连接的点数多，但扫描时间长。

6）当得到远程站信息则切断电源，结束执行配置模式。

7）设置面板 DIP 开关使 FX2N-64CL-M 转为在线（ONLINE）模式。

8）再次接通电源，并通过 FX2N-64CL-M 模块上的指示灯确认工作情况：如网络数据连接正常，则 L RUN 灯亮，否则 L ERR 亮或闪烁；如设置不正常，则 ERR 灯亮。

9）检查 FX2N-64CL-M 上的［BFM #0（0h）to #3（3h）］缓冲区确认远程模块是否连接。进而还可通过 PLC 外设监视从站工作。

10）编写程序，下载给 PLC，并起动系统运行。

（2）配置实例

本例网络如图 3-41 所示，有主站为安装有 FX2N-64CL-M 模块的 FX 系列机，从站，有

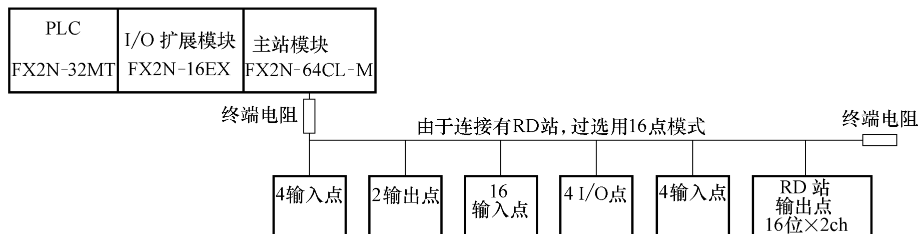


图 3-41　FX 机 CC-Link/LT 配置实例

4 点输入模块、2 点输出模块、16 点输入模块、4 点 I/O 混合模块、4 点输入模块及 RD 输出 16 位 *2 通道。还有电源、电源适配器等略。

按上述配置步骤配置。本例使用设置模式指定远程从站 I/O 地址。其他都制定了，但 RD 站没有指定。因为在缓冲区的 RD 处，分配有站址（49、50）。指定的结果见表 3-43 所示。

表 3-43　执行配置模式后本例 I/O 分配

	站类型	点数	指定 I/O(X)	指定 I/O(Y)	BFM
站 1	远程 I/O 站(输入)	4	X040 ~ X043	…	—
站 2	远程 I/O 站(输出)	2	…	Y020 ~ Y021	—
站 3	远程 I/O 站(输入)	16	X044 ~ X063	…	—
站 4	远程 I/O 站(输入、输出)	4	X064 ~ X065	Y022Y023	—
站 5	远程 I/O 站(输入)	4	X066 ~ X071	…	—
站 49	RD 站(输入)	16	…	…	208
站 50	RD 站(输出)	16	…	…	209
未使用 I/O			X072 ~ X077	Y024Y027	…

尽管这里没有上例各站中出现的空点，但最后 X072 ~ X077 及 Y023 ~ Y017 还是空闲点。因为这里 X\Y 编号虽与 Q 系列机不同，但它是以八进制推进的。最后的 X\Y 点不可能都能被 8 除尽，总有余数，余数部分就是所空出的点。本例输入总点数为 26 点，被除后余数为 6，故 X072 ~ X077 即为空闲的点。本例输出总点数为 4 点，被除后余数为 4，故 Y024 ~ Y027 即为空闲的点。

本例配置后的各站点输入输出点编号如图 3-42 所示。

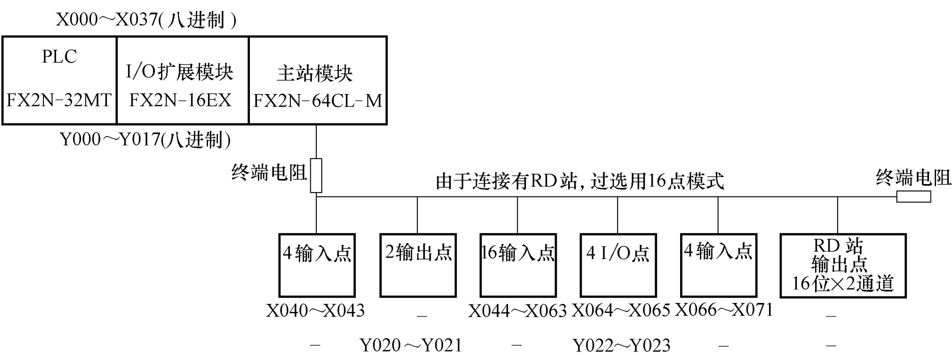


图 3-42　本例配置后各站输入输出点编号

当然，也可不用执行配置模式，而用设置缓冲区的方法来指定远程 I/O，只是太麻烦了。所以多不用它。有了上述地址分配，在应用程序中使用好这些地址，即可达到控制的要求了。如果用 FROM、TO 指令读写相关缓冲区，并用这些数据做输出或输入控制，则还可使网络的使用更加透明、工作更加安全。只是这些属于通信编程问题，这里略。

提示：从上两例可知，同样是 CC-Link/LK，但机型不同、模块不同，其配置是有区别的。所以，实际系统配置时，要具体问题具体对待。要参照说明书，按厂家的提示办。

3.4 CompoNet

关键词：TDMA、CIP、显式通信、隐式通信、5种工作模式、信息通信、远程I/O通信

CompoNet原始名称为“CipNet SA”，2006年4月，ODVA官方正式命名为此名。其产品由OMRON首先推出。CompoNet是用来在控制器（主站、Master）和传感器/执行器（从站、Slave）之间交换信息，主要针对“位”一级数据传输的执行器、传感器使用。是CIP网络家族（DeviceNet TM，ControlNet TM andEtherNet/IP TM）的补充，符合ODVA组织的行业标准。

本节先将对CompoNet网络作简要介绍，然后再对OMRON的CompoNet的组件及配置实例作具体说明。

3.4.1 CompoNet简介

1. CompoNet组成

图3-43所示为CompoNet网络组成示意。它有主站、远程I/O从站、中继器器、电缆及终端电阻。

（1）主站

为配置有CompoNet主站模块的PLC。在网络中，要有一个主站，也只能有一个主站。主站管理网络并发起与从站通信。主站除了循环地与从站远程I/O通信（Implicit，隐式通信），还可按需要与从站进行信息通信（Explicit，显式通信，只能1对1）。后者具有读取网络状态、配置网络工作的功能。同时，可连接配置有CompoNet插板的计算机。如果需要，CIP网络家族的其他层网络的相关站点也可与CompoNet的从站进行信息通信。

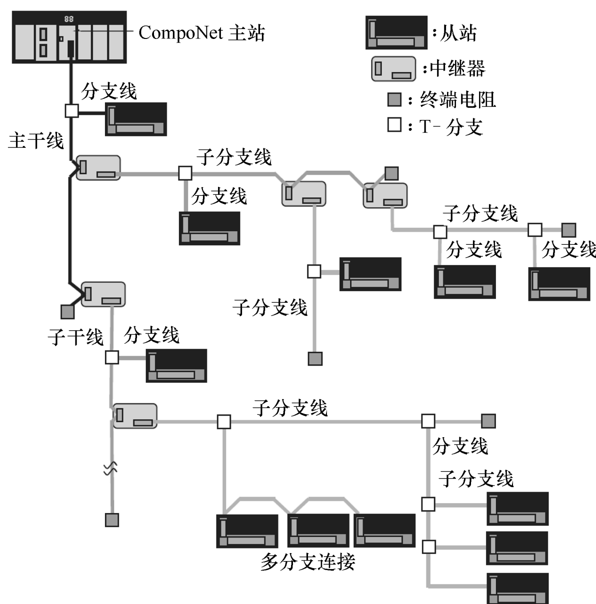


图3-43 CompoNet网络组成

（2）从站

可按需要配置，最多可达384个。从站类型有4种：

1）位从站单元。在CPU单元的I/O内存中，以2位为单位分配地址的从站。1个位从站单元提供2个或4个开关状态I/O点。位从站单元有IP20或者IP54防护等级的型号。

2）字从站：在CPU单元的I/O内存中，以16位（字）为单位分配地址。提供8个或更多开关I/O点。一个字从站还可安装1个扩展数字I/O模块，以增加I/O点数。

3）模拟量I/O从站。用于处理模拟量I/O值的从站单元。

4）智能从站。有一定数据处理能力的从站，如温度模块、通信模块等。

（3）电缆

为四芯专用电缆。其中两根用以传输信号，两根用以提供从站工作电源。使用的专用电缆有扁平电缆、一般圆形电缆及耐油高柔度圆形电缆等。

（4）网络附件

有与电缆对应的种种连接器及接线工具。还有中继器，既可用以延长网络传输距离，又可用以建立分支方便站点安装。网络最多可安装 64 个中继器。网络用的电源为 DC 24V 标准电源。可在网络的任何地方接入。此外，还有用于干线的远端接 1/4W、121Ω 终端电阻。

2. CompoNet 模型结构

对照 OSI 模型，它仅有 4 层，即物理层、数据链路层、传输网络层及应用层，如图 3-44 所示。

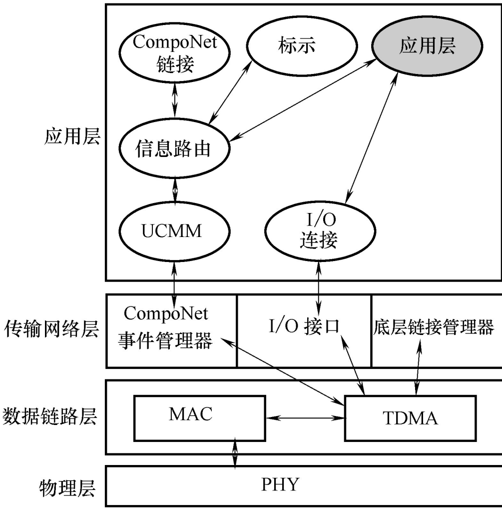


图 3-44　CompoNet 网络模型结构

（1）物理层

引用 RS-485 规范，使用曼彻斯特编码，并使用脉冲变换器（Transformer）做信号转换。脉冲变换器可使站点与电缆隔离，降低信号干扰，提高传输信号的可靠性。还可使传输的信号电压加倍，增加接收端信号幅值，便于接收端信号接收。此外，CompoNet 在接收端还使用数字信号滤波器进行接收屏蔽（Recevice mask），这种接收屏蔽还能增加抗拒尖峰电压与波形反射的能力，当信号幅值降低或畸变时，也能可靠地接收。

物理层还允许使用专用的中继器（Repeater）。使用它可延长干线距离，扩大网络控制范围与规模。可混用不同规格的电缆，主干线路可用圆电缆，而分支线路可用方便安装的扁平电缆。中继器可把网络分为多层（最多三层），分层加分支最多可使用 64 个中继器。

（2）数据链路层

它的 MAC 层用的是时域多址访问（Time Domain Multiple Access，TDMA，与本书第 1 章介绍的 TDMA 不完全一样）技术。具体是，网络主站点在每一轮询从站时，都会向各从站发送命令、数据及一个同步信号，用同步信号同步所有站点的时钟。在同步信号之后，每个站点在各自特定时间片内（如中间有中继器适当提前）发送响应数据，如图 3-45a 所示。

TDMA 技术与图 3-45b 所示的传统一问一答的探询通信相比，它没有或只有很小的通信间隙，在从站点较多时，通信效率要高得多。特别在有中继器时，它的这个优势更明显。因为数据经中继器时总要接收、整形，再发送，因而总要延时。而 CompoNet 使用的中继器是专用的，中继器（中继器也有地址）后的从站可认知自己的位置。这样，在使用 TDMA 技术时，中继器后的从站可根据自身在网络中的位置提前发送响应帧。这可补偿中继器的延时，实现即使用了中继器通信也无间隙。

但是，TDMA 技术要求各从站点都要配备一个有确定时间片长度的、稳定的时间基准及

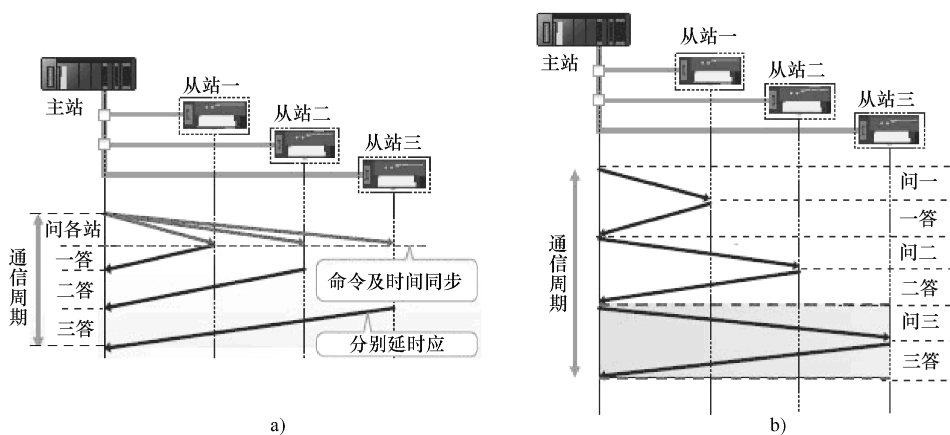


图 3-45　时域多址访问示意

能进行相应处理，价格也可能高些。TDMA 的另一个弱点是报文长度受时间片大小的限制。也因此它只适合像 CompoNet 这样远程 I/O 传输的网络。

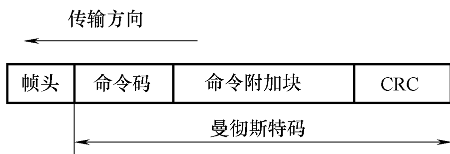


图 3-46　CompoNet 帧格式

CompoNet 网络的帧格式如图 3-46 所示。它有 4 部分组成：起始位，命令码，CRC 校验码。

CompoNet 定义的帧有 OUT、TRG、BEACON、CN、IN、A_EVENT、B_EVENT 7 种。其中 CN、IN 为从站所用。其他为主站所用。OUT 用于主站向从站写输出（O）数据。TRG 帧为主站向从站读数据。IN 用于从站向主站传输输入（I）数据。CN 为从站向主站相关命令的回应。BEACON 为主站通知从站它所使用的波特率。A_EVENT 为主站向从站发送显式数据。B_EVENT 为主站读取从站状态信息。等等。有了这些帧不仅可使主站与从站进行循环远程 I/O 通信、循时显式通信，还有便于网络的管理与诊断。

（3）传输与网络层

由于 CompoNet 应用层除了循环传送远程 I/O 数据，还有可跨网络的、循时显式信息传送。由于显式通信的报文可能较大，所以它才有不同于 AS-i、CC-Link/LT，用以处理网络桥接与路由及报文分割与重组的传输网络层。

CompoNet 使用 UCMM（Unconnected Message Manager）管理显式信息。在主站向从站发送显式信息通信之前必须先通知目标从站，为从站的 CN、CN 帧提供传输分时，进而使从站以参与的状态进入传输层。

主站通过 CN 帧检测现存的从站。当主站接收一个非参与状态从站的 CN 帧时，自动处理其为参与状态。这里的 STR（状态读）和 STW（状态写，由主站 B_EVENT 帧写）用作参与处理。显式信息（用 A_EVENT 帧）传送给处参与状态的从站。STW 告知从站执行 TDMA 要用到的“Cn Time Domain”、“ In Time Domain” 及“Out Block Pointer”。根据接收到的“Time Domain”告知，从站用一个 IN 和 CN 帧响应，然后重新读取主站 OUT 帧的数据。

参与处理之后，一个预定义的显式信息连接集生效。而当处参与状态的从站回应的 CN

和 IN 帧超过预定时间，主站则认为从站出现超时故障。

主站的 I/O 接口用于传送 TDMA 与上层网络之间的 IN 或 OUT 帧数据。而 IN 和 OUT 帧数据由 TDMA 自动更新。I/O 接口可取得 IN 数据，同时还为 TDMA 传送 OUT 数据。TDMA 通过 OUT 帧管理 OUT 数据分隔。I/O 接口可分隔由上层网络传来的 OUT 数据，使其转换为 TDMA 管理的格式。

CompoNet 事件管理器分割显式信息，也用其检测响应及重发送。CompoNet 事件管理器可缓存由上层网络送来显式信息。并在向 TDMA 发送要求之前，它把长帧分割为适合 TDMA 使用若干较小的帧。

TDMA 收到显式信息响应会告知 CompoNet 事件管理器。当事件管理器接收分割的若干小帧时，会将其重组为显式信息响应，并把重组的信息传输给上层网络。管理器还会检测此响应是否超时。如果超时，管理器或重发信息，或把从站处理为超时故障。

（4）应用层

也是网络高层。涵盖 OSI 模型表示层以上的各层。它使用 ODVA 开发的共同工业协议（Common Industry Protocol，CPI）。这协议是通用的应用层开放的协议、与具体网络硬件无关的协议。这意味着它能用于很多不同的网络，不仅是 CompoNet 的高层协议，也还是 ODVA 管理下的 DeviceNet、ControlNet 及 EtherNet 的高层协议。它允许报文能够毫无阻碍的从 EtherNet/IP 到 ControlNet 再到 DeviceNet。近期，CIP 协议的两个扩展协议 CIPSafety 和 CIPSync 也成功地运用在 EtherNet/IP 上，这样通过 EtherNet/IP 就可实现安全网络和高精度时间同步应用。可通过 EtherNet/IP 实现分布式运动控制应用。

CIP 是严格面向对象的协议。每个 CIP 对象都有属性（数据）、服务（命令）及行为（事件反应）。CIP 还定义部件类型，其中含部件设置描述。这个描述指明该部件类型的对象集合、配置选项及 I/O 数据格式。这样的好处是，在 CIP 网络上，使该类型部件时都有一个公用的应用接口，很便于不同厂家同类型产品的相互操作。这些产品如有特殊之处，还可另定义特殊对象，去支持其特殊增加的功能。

无缝桥接与路由可使从一个网络接口得到的数据，传递到另一个网络接口。这是 CIP 最重要的优点。这无缝桥接与路由只是使能已定义一组“路由机制”的对象。用户的责任仅仅是描述信息传送必须遵循的路径。之后 CIP 将正确地处理这个信息，而不管 CIP 所属的下层具体网络，进而可确保在这个路由过程中信息内容不被改变。

此协议落实到 CompoNet，定义 CompoNet 的通信主要是远程 I/O 通信。这对 PLC 设备网或现场总线，如同 AS-i、CC-Link、LT 一样，是最基本的通信。此外还有显式通信。这是前两个网络所没有的。对 OMRON PLC 这显式通信还可使用 OMRON 的 FINS 协议。

3. CompoNet 拓扑结构

CompoNet 为总线结构。一般使用干线（Trunk Lines），指主站与终端电阻之间的传输路径。也可使用中继器延长干线，延长的部分称子干线（Sub-trunk lines），为中继器与终端电阻之间的传输路径。也可从主干线或子干线分支建立传输路径，称之为分支线（Branch Lines）。也还可再从分支线分支建立传输路径，称之为子分支线（Sub-branch Lines）。具体总线结构如图 3-47 所示。有关限制条件见表 3-44。

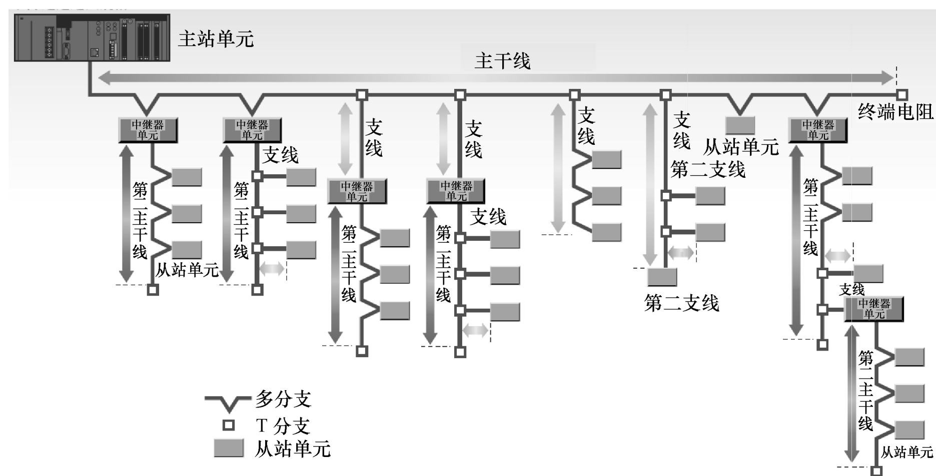


图 3-47　CompoNet 拓扑结构

表 3-44　拓扑结构使用的限制条件

■ 限制条件（波特率 4Mbit/s（无分支线））

电缆类型	每段最大长度（带中继器单元的最大长度）	每段分支线长度	每段分支线长度合计	分支位置限制条件	每段最大从站单元数②
圆形电缆Ⅰ	30m(90m)	0m①	0m①	—	32 节点
扁平电缆Ⅰ,扁平电缆Ⅱ,及圆形电缆Ⅱ	30m(90m)	0m①	0m①	—	32 节点

① 不能连接 T 分支（只有多分支连接时可以）。
② 节点数包括中继器单元。

■ 限制条件（波特率 3Mbit/s）

电缆类型	每段最大长度（带中继器单元的最大长度）	每段分支线长度	每段分支线长度合计	分支位置限制条件	每个分支的最大节点数①	每段子分支线长度	每段子分支线长度合计	每段最大从站单元数②
圆形电缆Ⅰ	30m(90m)	0.5m	8m	3 分支/m	1 节点	0m	0m	32 节点
扁平电缆Ⅰ,扁平电缆Ⅱ,及圆形电缆Ⅱ	30m(90m)	0.5m	8m	3 分支/m	1 节点	0m	0m	32 节点

① 每个分支的最大节点数是可以连接到一个多分支或 T 分支（子分支）的最大从站单元数或中继器单元数。
② 节点数包括中继器单元。

■ 限制条件（波特率 1.5Mbits/s）

电缆类型		每段最大长度（带中继器单元的最大长度）	每段分支线长度	每段分支线长度合计	分支位置限制条件	每个分支的最大节点数①	每段子分支线长度	每段子分支线长度合计	每段最大从站单元数②
圆形电缆Ⅰ	无分支	100m(300m)	0m③	0m③	—	—	—	—	32 节点
	有分支	30m(90m)	2.5m	25m	3 分支/m	3 节点	0m	0m	32 节点
扁平电缆Ⅰ,扁平电缆Ⅱ,及圆形电缆Ⅱ		30m(90m)	2.5	25m	3 分支/m	3 节点	0.1m④	2m④	32 节点

① 每个分支的最大节点数是可以连接到一个多分支或 T 分支（子分支）的最大从站单元数或中继器单元数。
② 节点数包括中继器单元。
③ 不能连接 T 分支（只有多分支连接时可以）。
④ 从分支线过来的 T 分支连接。

（续）

■ 限制条件（波特率 93.75kbit/s）

电缆类型	每段最大长度（带中继器单元的最大长度）	每段分支线长度	每段分支线长度合计	分支位置限制条件	每个分支的最大节点数①	每段子分支线长度	每段子分支线长度合计	每段最大从站单元数②
圆形电缆 Ⅰ	500m（1500m）	6m	120m	3 分支/m	1 节点	—	—	32 节点
扁平电缆 Ⅰ，扁平电缆 Ⅱ，及圆形电缆 Ⅱ	每段总长度为 200m 没有限制条件							32 节点

① 每个分支的最大节点数是可以连接到一个多分支或 T 分支（子分支）的最大从站单元数或中继器单元数。
② 节点数包括中继器单元。

4. CompoNet 主要规格

表 3-45 所示为 CompoNet 的主要规格。

表 3-45　CompoNet 主要规格

项　　目	说　　明
通信类型	远程 I/O 通信（无须编程，常与从站共享数据）和信息通信（按要求与从站显式通信）
波特率	4Mbit/s，3Mbit/s，1.5Mbit/s，93.75kbit/s
调制	基带
编码	Manchester 码
纠错	CRC
最大 I/O 容量	字从站：1024 输入和 1024 输出（2048 I/O 总点数） 位从站：256 输入和 256 输出（512 I/O 总点数）
最多站点数	字从点：64 输入和 64 输出站点 位从站：128 输入和 128 输出站点 中继器：64 站点
每站点占用位数	字从站：16 位 位从站：2 位
每干线可连接的站点数	32 站点（含中继器）
中继器应用条件	每主站可连接 64 个。每主（含子）干线可连接 32 个。当与主站串联连接时，只允许在主站与从站之间只能有 2 个中继器。

5. CompoNet 特点

1）容量大、速度快。可连接 384 个从站，最多可控制 2560 I/O 点。通信速率高（最高速率达 4Mbit/s），响应时间短，1000 点 I/O 扫描时间可小于 1ms。

2）安装灵活、接线方便。站点可分散分布，位从站使用可更分散布线。可使用专用电缆，快速接线。当波特率为 93.75kbit/s 时，网络最大距离可达 1500m。

3）设置简单。只要设置好主站模式及波特率，设置好各从站地址，连好线就可运行。不要软件配置。

4）使用方便。从站可带电退出与接入网络。

5）内置智能功能。有完整的状态显示，可方便进行网络故障快速诊断。也可用 CompoNet 支持软件帮助检测接线错误、电源失效及其他故障。使用中继器做网络分段，还可即使出现故障还可隔离，不至于整个网络瘫痪。故障还可予以记录，可保持有关历史数据。图 3-48 所示为上述功能的图解示意。

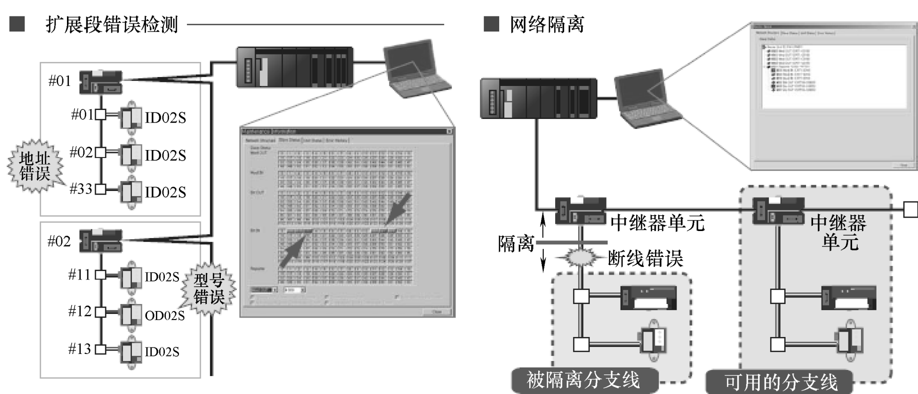


图 3-48　智能功能图解示意

6. 全球化公开网络

有国际标准支持，应用广泛，特别适用于如下 3 种场合：

1）站点分散，分布面广的制造业生产线。

2）大型多传送带传送控制。

3）大型立体仓库控制。

3.4.2　OMRON CompoNet 组件

1. CJ1、CS1 机用主站模块

CJ1、CS1 机为近期 OMRON 开发的中、大型机。性能优越。OMRON 首先选用它开发 CompoNet 主站模块，也是 OMRON PLC 唯一具有的主站模块。

（1）外观

两机型模块外观基本相似，如图 3-49 所示。

从图知，其面板上有：显示部分、旋转开关设定部分、DIP 开关设定部分、通信电源接口及通信连接器。

1）显示部分。有指示灯 MS（绿/红）、NS（绿/红）、SD（黄）及 RD（黄）显示及两个 7 段数字码 + “.” 号（可显示 +100）显示。这些可显示网络通信状态及出错代码。指示灯显示含义见表 3-46，7 段数字显示含义见表 3-47。

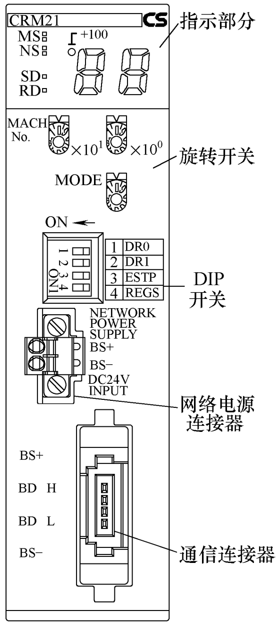


图 3-49　主站模块面板外观

表 3-46　指示灯显示含义

指示灯	状态	状态名称	含　　义
MS	亮(绿)	正常	模块操作正常
	亮(红)	严重故障	模块硬件出错,诸如看门狗监视超时
	闪烁(红)	非严重故障	通信模块数或单元号设置错
	不亮	电源不工作	电源 OFF,正位或初始化
NS	亮(绿)	在线,处于远程站通信过程	供电正常,远程 I/O 已开始通信,无从站及中继器出错,无登记表出错,无从站及中继器地址重复

（续）

指示灯	状态	状态名称	含　　义
NS	闪烁(绿)	在线，未与远程站通信	远程通信为启动或非通信出错引起的停止
	亮(红)	严重通信出错	通信线路出错
	闪烁(红)	非严重通信出错	一个或多个从站或中继器通信出错。一个或多个从站确认出错(由于从站没有登记或不存在)。由于通信出错引起通信停止。组态出错(中继器数量)。从站或中继器地址重复
	不亮	电源不工作	电源 OFF，正位或初始化
SD	亮(黄)	正常发送	主站正常发送帧
	不亮	不发送	主站不发送数据
RD	亮(黄)	正常接收	主站正常接收帧
	不亮	不接收	主站不接收数据

表 3-47　7 段数字显示含义

状　　态		显示内容	显示	实际显示	内　　容
正常	远程 I/O 通信	波特率显示亮	_0	亮	4Mbit/s
			_1	亮	3Mbit/s
			_2	亮	1.5Mbit/s
			_3	亮	93.75kbi/s
	远程 I/O 通信停止	波特率显示闪烁	_0	闪烁	4Mbit/s
			_1	闪烁	3Mbit/s
			_2	闪烁	1.5Mbit/s
			_3	闪烁	93.75kbit/s
出错	初始化出错	出错码	十六进制显示(亮)		
	通信出错	出错码，从站类型，站点地址交替显示	出错码(两位十六进制数)，从站类型和站点地址交替显示		

举例	出错码 显示	出错码 实际显示	从站类型 显示	从站类型 实际显示	含义
发生一个通信出错	d9		i		输入
			o		输出
			bi		位输入
			bo		位输出
			r		中继器
站点地址重复错	d0		同上		
出现不存在站点错	d5		同上		
非登记从站确认错	d6		同上		

（续）

<table>
<tr><th colspan="2">状 态</th><th>显示内容</th><th>显示</th><th colspan="2">实际显示</th><th>内 容</th></tr>
<tr><td rowspan="6">出错</td><td rowspan="6">运行出错</td><td rowspan="6">出错码</td><td colspan="4">二进制显示出错码(亮)</td></tr>
<tr><td rowspan="2">举例</td><td colspan="2">出错码</td><td rowspan="2">—</td></tr>
<tr><td>显示</td><td>实际显示</td></tr>
<tr><td>由于通信出错停止通信</td><td>A0</td><td></td><td>…</td></tr>
<tr><td>软件数据设置非法</td><td>E4</td><td></td><td>…</td></tr>
<tr><td>登记表数据非法</td><td>E8</td><td></td><td>…</td></tr>
</table>

2）旋转开关设定部分。有两组。其中一组两个用以设定主站模块的机号，允许在 0 ~ 99 之间设定（仅 0 ~95 有效）。另一组一个，用以设定工作模式。可在 0 ~9 之间设定（仅 0 ~3 及 8 有效）。

3）DIP 开关设定部分。有两组 4 个。其设定含义见表 3-48。

表 3-48　DIP 开关设定含义

SW1	SW2	波特率
DR0	DR1	
OFF	OFF	4Mbit/s(default)
ON	OFF	3Mbit/s
OFF	ON	1.5Mbit/s
ON	ON	93.75kbit/s

SW	名 称	ON	OFF
3	ESTP(通信出错停止模式)	当通信出错时停止	当通信出错时不停止
4	REGS(登记表使能设定)	使能	不使能

4）通信电源接口。用以连接 DC 24V 电源。

5）通信连接器。用以连接通信电缆。BS +，BS –（通往从站的通信电源线）和 BDH，BDL（通往从站的通信数据）。

（2）工作模式

有 5 种工作模式。不同模式所占的单元号、控制从站数及使用的内存区是不同的。具体如表 3-49 所示。

表 3-49　不同工作模式特性

<table>
<tr><th>通信模式</th><th>名称</th><th>连接站点地址</th><th>控制点数</th><th>内存区</th><th>每主站使用的单元号数</th></tr>
<tr><td>0</td><td>通信模式 0</td><td>字从站：
输入 0 ~7 输出 0 ~7</td><td>字从站单元：
128 输入、128 输出</td><td rowspan="4">特殊 I/O 单元区（首字取决于单元号）</td><td>2</td></tr>
<tr><td>1</td><td>通信模式 1</td><td>字从站：
输入 0 ~15 输出 0 ~15</td><td>字从站单元：
256 输入、256 输出</td><td>4</td></tr>
<tr><td>2</td><td>通信模式 2</td><td>字从站：
输入 0 ~31 输出 0 ~31</td><td>字从站单元：
512 输入、512 输出</td><td>8</td></tr>
<tr><td>3</td><td>通信模式 3</td><td>字从站：
输入 0 ~15 输出 0 ~15
位从站：
输入 0 ~63 输出 0 ~63</td><td>字从站单元：
256 输入、256 输出
位从站单元：
128 输入、128 输出</td><td>8</td></tr>
</table>

（续）

通信模式	名称	连接站点地址	控制点数	内存区	每主站使用的单元号数
4	保留	…	…	…	…
5	保留	…	…	…	…
6	保留	…	…	…	…
7	保留	…	…	…	…
8	软件设置模式	可在以下范围设置： 字从站： 输入 0 ~ 63 输出 0 ~ 63 位从站： 输入 0 ~ 127 输出 0 ~ 127	可在以下范围设置： 字从站： 1024 输入、1024 输出 位从站： 256 输入、256 输出	可在 CIO、DM、WR 或 HR 区任意分配 提示：状态写参数分配在特殊 I/O 单元区	1
9	保留				

（3）内存地址

与从站地址有关。CompoNet 从站有输出字站点、输入字站点、输出位站点、输入位站点及中继器站点。这 5 种站点都要分别设定地址。字从站与中继器的最大地址范围为 0 ~ 63，位从站最大地址范围为 0 ~ 127。各自设的地址不重复就可以了。

对模式 0 ~ 3，主站与从站交换数据使用 PLC CPU 单元的内存区，即 CIO 2000 ~ 2959。具体与主站模块的单元号设定有关。其开始地址为：CIO 2000 +（10 x 单元号），要占多少字与工作模式有关。而单元号可以是：0 ~ 95，由面板上的两个旋转开关设定。各个站点占用的内存地址与该站点地址有关。站址 0 在最前面，其余按站点号升序依次排列。先是输出区，继而为输入区，最后为状态与设定区。图 3-50 所示为工作模式 0（8 个字输出从站、8 个字输入从站）的内存区分配实例。

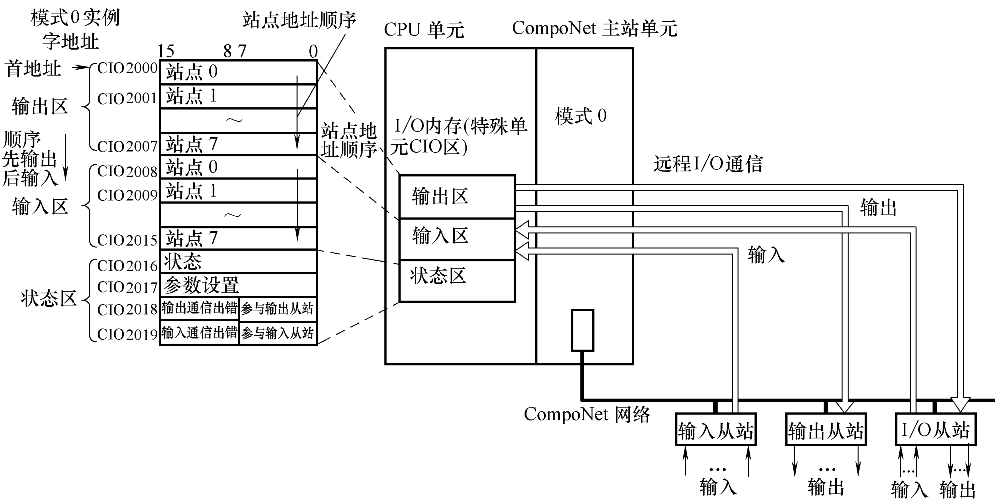


图 3-50　模式 0（8 个字输出从站、8 个字输入从站）内存区分配实例

工作模式 8 功能最强，为软件模式，所控制的从站点最多，所占用的地址也最多。其开始地址可指定 CPU 单元的 CIO、WR、HR、或 DM 区的想要使用的地址。但内存地址要用编

程软件的主站单元 I/O 分配的标签页，分别在 CIO，DM、WR 或 HR 区，指定字输出、字输入、位输出、位输入及状态区的首地址。图 3-51 所示即为它的设定示意。

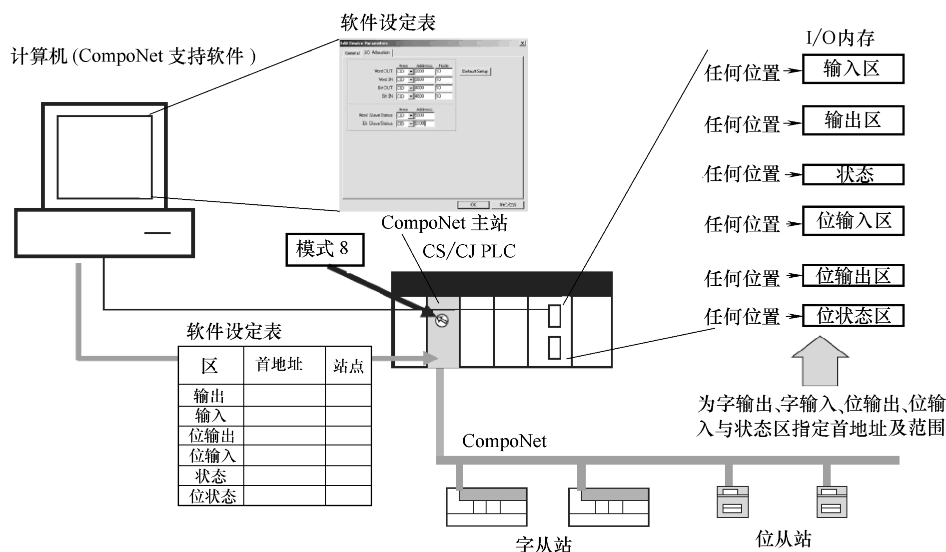


图 3-51 模式 8 设定示意

（4）通信实施

有远程 I/O 通信及信息通信：

1）运程 I/O 通信。有了从站状态信息及从站所占用的地址，远程通信实施就很容易了。状态信息包含 3 方面内容：网络与主站模块状态；远程 I/O 通信起动开关；可应用的从站参与标志及通信出错标志。具体内容及其地址与工作模式有关，可参阅主站说明书。至于如何利用这状态信息，可参阅图 3-52 实例。

从图知，这里利用所分配的 I/O 地址的前提是，常开触点 a 必须 ON。而 a ON 的条件是“梯形图操作允许位”ON。而这个 ON 的条件是：登记表使能允许，并已登记的从站全部在网上；远程 I/O 通信已运行；通信无误。

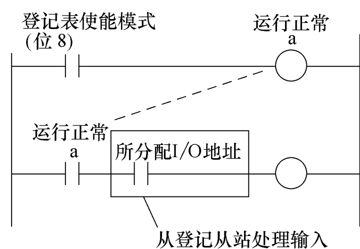


图 3-52 状态信息处理实例

2）信息通信。有 CompoNet Explict 通信及 OMRON 的 FINS 通信，其功能是发送与接收在 PLC CPU 单元与主站单元之间以及 PLC CPU 与 CompoNet 从站单元之间的数据，如时间或出错历史信息，强制置位、复位操作。信息通信按用户要求设计，只要执行条件满足即执行。

OMRON 的 FINS 通信由 OMRON 公司开发，适用于 OMRON PLC 从站。但它的通信命令（CMND 命令码 3802）也可执行 CompoNet Explict 通信。

CompoNet Explict 通信使用的为 CIP 网络通信协议。远程设备可以是 CompoNet 从站。FINS 通信可跨 OMRON 网络，最多 3 层。而 CompoNet Explict 通信也可跨网络。有关细节是通信编程问题，这里略。

2. 计算机用主站插板

有 3G8F7-CRM21 PCI 型及 3G8F8-CRM21 紧凑 PCI 型插板。安装后用于 WINDOWS 或兼容操作系统，分享计算机内存区。可使用 C/C + +/VB 编程。

3. 网关模块 GQ-CRM21，可用以把 CompoNet 从站接入 CC-Link

4. 从站

OMRON 提供的 CompoNet 从站单元有多种类型与规格，分别适用于不同分布应用场合。用户可根据应用需要选择。从规格说有：

（1）字从站单元

有基本单元与扩展单元。后者可与前者连接以扩展站点的 I/O 点数。但每个基本单元只能接一个扩展单元。在 CPU 单元的 I/O 内存中以 16 位（字）为单位分配地址的从站单元。具体单元见表 3-50。

表 3-50　字基本单元与扩展单元

名　称	型　号	规　格
基本单元	CRT1-ID16	16DC 输入(NPN)
	CRT1-ID16-1	16DC 输入(PNP)
	CRT1-OD16	16 晶体管输出(NPN)
	CRT1-OD16-1	16 晶体管输出(PNP)
扩展单元	XWT-ID08	8DC 输入(NPN)
	XWT-ID08-1	8DC 输入(PNP)
	XWT-OD08	8 晶体管输出(NPN)
	XWT-OD08-1	8 晶体管输出(PNP)
	XWT-ID16	16DC 输入(NPN)
	XWT-ID16-1	16DC 输入(PNP)
	XWT-OD16	16 晶体管输出(NPN)
	XWT-OD16-1	16 晶体管输出(PNP)

（2）模拟量 I/O 从站单元

有 CRT1-AD04 模拟量输入单元，可输入 4 路模拟量。有 CRT1-DA02 模拟量输出单元，可输出 2 路模拟量。

（3）位从站单元

有 IP20 或 IP54 防护等级的型号。点数多为 2 点、个别为 4 点。2 点的或输入点，或输出点。4 点的，或为输入点，或混有输入输出点。在 CPU 单元的 I/O 内存中以 2 位为单位分配地址的从站单元。

（4）智能从站单元。有智能 CompoNet 通信单元、CompoNet 传感器通信单元等。

5. 附件

有 CRS1-RPT01 中继器（Repeater Unit），可与不同类型的电缆连接器。有 DCN4-TM4、DCN5-TM4、DRS1-T 不同型号的终端电阻，分别可与不同的电缆连接。还有电缆及相关的连接器及连接操作工具。等等。

3.4.3　OMRON CompoNet 配置实例

以下用实例说明 CompoNet 网络配置及其实际使用过程。系统配置如图 3-53 所示。其配

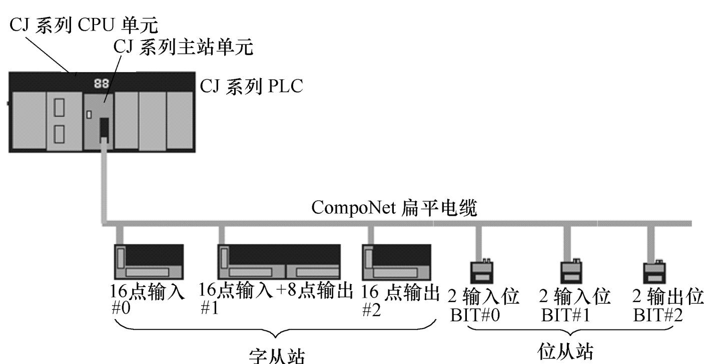


图3-53　系统配置

置先是脱机用软件设置，然后联机把设置下载，并监视。

1. 脱机设置

要运行CX-Integrator软件。该软件集成在OMRON CX-One软件包中。具体步骤如下：

1）创建新工程，建立仅有主站的网络。所建立的网络选定CompoNet。选定后将弹出如图3-54所示的“向导-主单元”窗口。



图3-54　新工程及“向导-主单元”窗口

出现后按图上提示，本例主单元选定为“CJ1G-CPU45”。进而点击“下一步”按钮。将弹出如图3-55所示仅有主站网络的窗口。

2）添加从站点。可在图4-34新工程窗口的左下方组件类型的小窗口上，点击“DTM（CompoNet）”标签，在出现的“DTM（CompoNet）”表单上，再点击“DeviceNetType”处“+”号，将其目录展开。进而用鼠标从展开的目录中选择所需要的从站部件，并把它拖放到仅有主站的网络上。本例拖放了3个字从站，3个位从站。如图3-56所示。

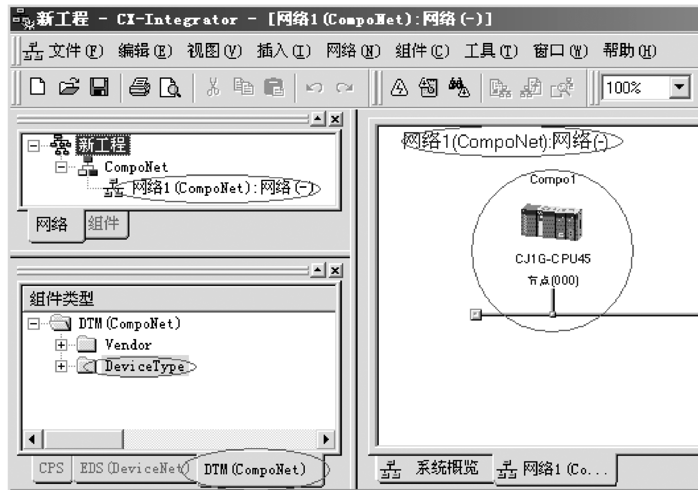


图 3-55　仅有主站网络

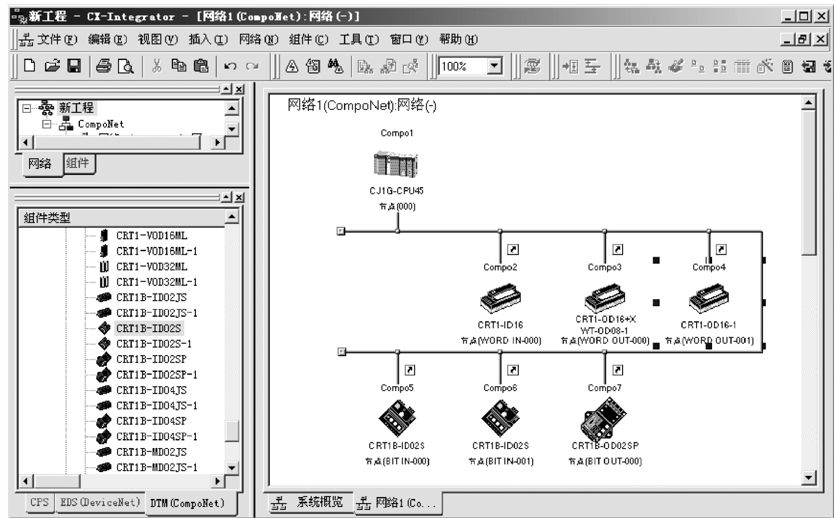


图 3-56　3 个字从站 3 个位从站

3）设置各个从站点。可双击各个从站点图标，将弹出该从站点的设置（Configuration）窗口。可根据需要做有关设置。图 3-57 所示为 CRT1B-OD02SP 从站配置窗口。

其上有 3 个表单，该图显示的是输出设置表单，可对其设置 00、01 输出点出错及空闲处理。本例选择 00 点位保持（输出状态不变），01 点清除（输出转为 OFF）。其他表单及其他站点如需要也都可做设置。当然也可不设置直接采用缺省值。



图 3-57　CRT1B-OD02SP 从站配置窗口

4）登记注册表。确定主从站关系。为此，

要双击主站图标。击后将弹出如图 3-58 所示，主站设置窗口通用表单。

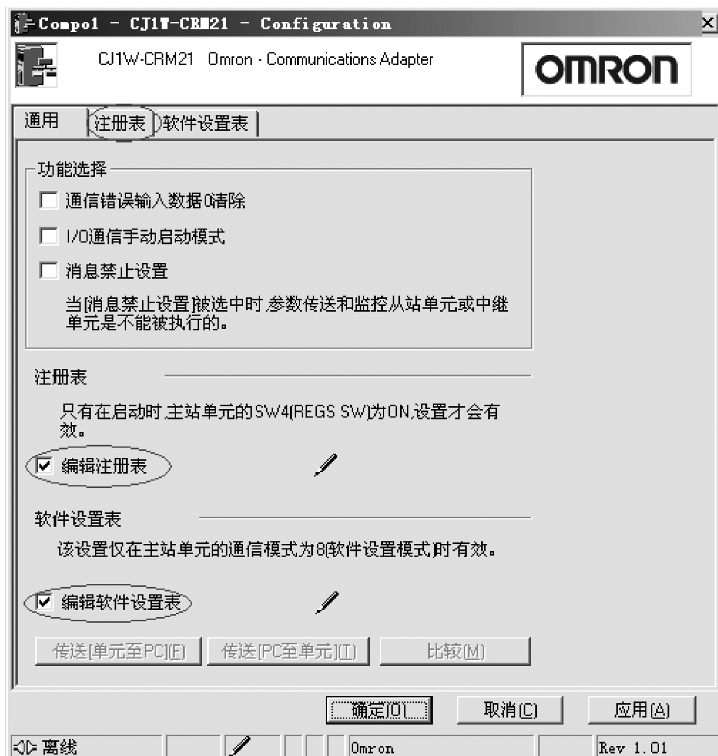


图 3-58　主站设置窗口通用表单

之后，要在其上点击图示“编辑注册表”及“编辑软件设置表”项（打“勾号”）。表明要对这两项做编辑。选定后，才显示有这两项标签。这时点击图示“注册表”标签，将出现图 3-59 所示“注册表”表单。

该窗口已注册了 4 个从站，还有两个待注册。图示已选定#00 从站（颜色已加深）。这时如点击向下箭头按钮，将把#00 从站从未注册设备列表中转记入已注册设备列表中。本例都应把所有从站转记入已注册设备列表中。此外，打开软件设置表还可做相应设置。这些设置全部完成后，可点击确定，则完成了脱机设置。



图 3-59　“注册表”表单

2. 联机下载设置及网络监视

为此，先要实际接线、安装、联机及下载上述设置，然后进入监视画面进

行监视。其过程如下：

1）按图 3-60 要求接线。

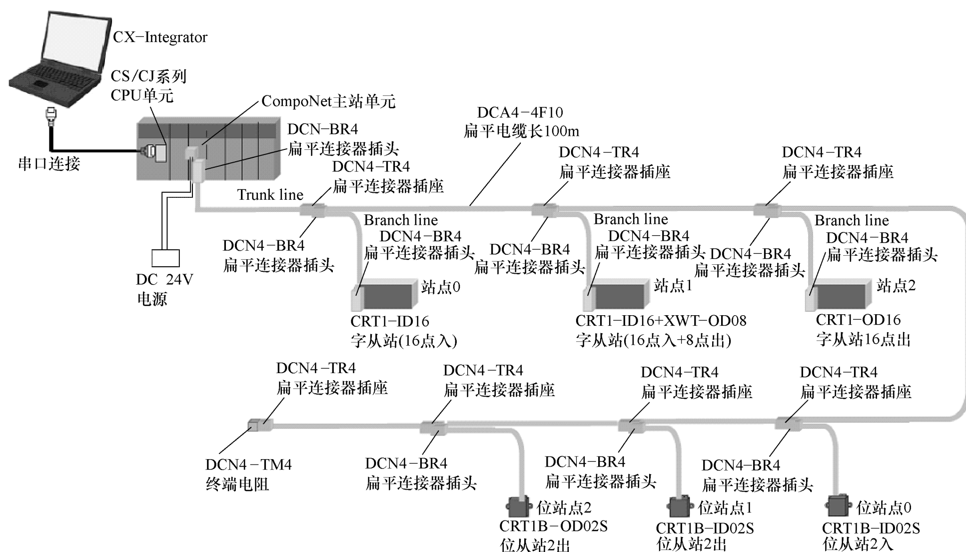


图 3-60　接线要求

2）主站设定通信模式。用主单元面板模式旋转设定。本例设定为模式 3，允许字输入、输出站点各 16 个，位输出个点，位输入、输出站点各 64 个。

3）设定波特率及登记表使能、通信出错处理。用面板上 DIP 开关设定。本例波特率为 3Mbit/s，登记表使能设定为使能、通信出错处理设定为出错停止。

4）设定主站的单元号。本例设定为 5，所使用内存区起始地址为 CIO 2050。

5）设定从站地址。本例设定 CRT1-ID16 字站点地址为#0，CRT1-ID16 + XWT-OD08 字站点为#1，CRT1-OD16 字站点地址为 #2，CRT1B-ID02S 位站点地址为#0，CRT1B-ID02S 位站点地址为#1，CRT1B-OD02S 位站点地址为#2。

6）计算机运行 CX-Integrator OMRON 网络管理软件，并通过串口与 PLC CPU 模块串口连接。

7）PLC 接通电源。

8）使 CX-Integrator 软件在线，编辑并下载上述主单元设置。

9）PLC 断电再上电使上述设置生效。

10）网络通信开始。这时如从站全已连接、工作正常，面板上 MS、NS 指示灯显示绿色。如出错将有不同显示，而且在面板 7 段数字将显示相关错误代，从中可得到相关出错信息。进而可做适当处理，把故障排除。

11）用 CX-Integrator 监视联网的从站状态。用鼠标右击主站图标，在弹出的下拉菜单上选择“监视”项，将弹出监视部件窗口。该图正监视从站参与状态绿色为参与，红色为断开，灰色为未参与连网。而要监视主站状态可点击“Unit Status”表单项。之后将显示主站状态画面，可用以监视主站。

第 4 章　PLC 控制网配置

PLC 控制网主要用于 PLC 独立站点间的数据交换与相互操作。但多数 PLC 控制网还可用于 PLC 与计算机间进行通信。同时，还多有远程 I/O 系统，可与远程设备通信。运用 PLC 控制网可扩大 PLC 的控制地域及增大控制规模；可实现 PLC 控制的综合与协调；可提高 PLC 控制的可靠性。同时，更便于实现 PLC 冗余配置。

本章将对 PLC 控制网的发展及配置作简要介绍。

4.1　PLC 控制网概述

关键词：专用 PLC 控制网、基于标准的 PLC 控制网

PLC 控制网的特点是：可靠性要求高，不能出现差错；实时性要求高，通信时延要确定，也不能太长；通信的数据量可能不太大；目前正从封闭走向开放。

4.1.1　专用 PLC 控制网

早期，PLC 控制网都是专用的。各公司各有自己的专用网络，互不开放，只能用于本公司的 PLC 产品接入。同时，每个公司还有多种不同性能的这样的网络。如 OMRON 公司的 PLC-LINK、SYSMAC Link、SYSMAC NET Link，三菱公司的 MELSECNET/10（H）网，西门子公司 S5 机的 L1、L2 网络，等等，就是典型的 PLC 专用控制网络。以下以 OMRON 的 SYSMAC Link 网络对此作简要说明。

SYSMAC Link 网络可配置成单级的，即所有的 PLC 仅接插一个 SYSMAC link 单元，并通过同轴电缆或光纤进行连接，以形成多个站点的总线网。单级的最大站点数为 62。也可配置成多级的，即有的 PLC 接插两个 SYSMAC Clink 单元，分别与其他 PLC 的 SYSMAC link 单元连成各自的子网。最多可配置成 128 级。多级网络中的各个级，最大站点数也都可为 62。图 4-1 所示的就是 OMRON 的 SYSMAC Link 网络的几种配置。

这里，图 4-1a 为单级结构配置。所有站点仅使用一个 SYSMAC link 单元，用同轴电缆或光纤进行站点间的物理连接。图 4-1b 也为单级的，但用同轴电缆的联网。与图 4-1a 不同的是它附加有备份电源，以实现站点旁路，即若该站点出现故障，只要仍有电源，不影响后续站点正常工作。图 4-1c 为三级网络，因为其上有两个 PLC 装有两个 SYSMAC link 单元。

从图可知，要想把 PLC 接入此网络，得有 SYSMAC Link 单元。不同型号 PLC 所用的单元也不相同。如 CV500 机，有 CV500-SLK11 及 CV500-SLK21 单元。前者用于光纤网，后者用于同轴电缆网。对光纤单元还要附加电源辅助电源单元。所以，其他厂家的 PLC 是无法接入的。

SYSMAC Link 网的数据传送速率可达 2M 波特率。若使用同轴电缆作通信介质，总计传送距离可达 1km。若使用电缆作通信介质，其站点间的传送距离可达 800m，总距离可达 10km。

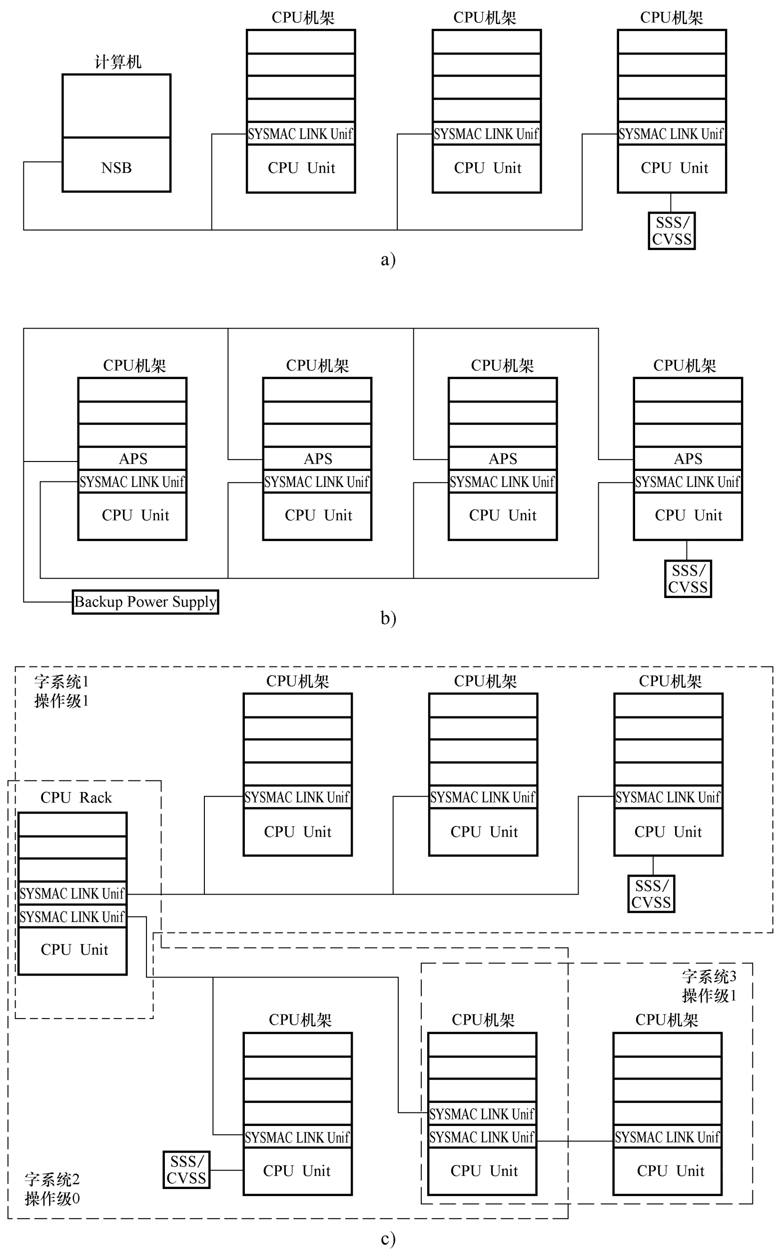


图 4-1 OMRON SYSMAC Link 网

SYSMAC Link 网实现通信有两种方法，一为数据链接，另一为执行通信指令。数据链接是用指定的数据链接区自动交换数据，链接区含 LR 继电器及 DM 区，可人工设定，容量大，而且灵活。执行通信指令有数据读（RECV）、数据写（SEND）及命令发送（CMND）3 条指令。其方式有：广播传送，可向网上所有站点发送数据；指定通信站点号，并设定响应的时间；可使用传送重试设定；可禁止或使能响应；等等。但要通过运行程序才能执行这些指令。SYSMAC Link 是令牌总线网。哪个站点拥有令牌，哪个站就拥有总线，哪个才可发送数据。

在 SYSMAC Link 网上，有一站点号最小的单元，称为呼叫单元（Polling unit），管理令牌，控制网络通信。如果该站点出现故障，则其相邻的次低站点号的站点，自动成为呼叫单元，控制网络通信，以避免使整个网络瘫痪。

此外，在 SYSMAC Link 网上，还有一个起始站点（Startup Node），由它设定内存区控制字的内容，起始或停止网的数据链接。在人工设定数据链接区时，也由它设定有关通信参数。指定哪个站点为呼叫单元及起始站点，由软设定（Software Setup）确定。

通信过程是周而复始、循环进行的。每一周期由两部分组成：令牌周期（Token Cycle）及呼叫周期（Polling Cycle）。

令牌周期：令牌首先通过呼叫单元，依次由低号站点流向高号站点，直到最高号后又回到呼叫站点，这一完整的循环过程，称为令牌周期。

呼叫周期：每次令牌周期结束后，呼叫单元控制网络上是否有新的站点加入，或原有站点移出，并把检测出的最新信息传送给各个站点。这个检测及传送过程，称为呼叫周期。令牌周期与呼叫周期的组合，即为通信周期，它是网络工作的重要参数。此外，网络还有其他参数，如：被呼叫的站点数，最大帧数，最大站点地址。这些参数也要作设定。

如果要求计算机业接入 SYSMAC Link 网，就要在计算机中插入 SYSMAC Link 支持板及其组件，并通过同轴电缆或光缆与总线与其他站点相连。进网的计算机与其他 PLC 可通过数据区链接，自动进行数据交换，也可使用 OMRON FINS 协议的通信命令与指定的 PLC 通信、交换数据，还可使用 OMRON 提供的软件对 PLC 编程、设定及对其工作监控。

此外，OMRON 开发的工厂智能终端（FIT）通过 PLC 的外设接口（也是 OMRON 开发），与 PLC 相连也可用对网上任一 PLC 编程或监控。

总之，这样的专用网络，性能虽然还可以，但一切包括软件都要用 OMRON 的产品，完全是封闭的。封闭的结果必然是，厂家的产量不大，生产成本高；用户使用时，造价也就高，要熟悉一个个不同的专用网络也很不容易，至于维修、部件更换就更不便了。所以，这样封闭的网络已逐步被开放的、基于行业标准的网络所取代。因而本书也不对这样的网络作进一步介绍。

4.1.2　基于标准的 PLC 控制网

这里讲的基于标准的 PLC 控制网络是指符合本书第 1 章介绍 PLC 事实标准的网络。具体是 CC-Link、DeviceNet、ControlNet 及 Profibus。这些网络具有现场总线的特点，如不是一 PLC 厂家专用，而是多个 PLC 厂家共享；协议公开，任何符合协议的产品都可入网；网络性能高，技术进步快，不断有新的产品推出；使用面广，产品可批量生产、价格低，网络组建成本低；也具有设备网的功能，可与从站实现远程 I/O 通信；可与设备网、信息网无缝连接，便于实现企业控制的信息化，等等。正是这些特点，本书 PLC 控制网一章将仅对这些网络分节作较具体介绍。

4.2　CC-Link

关键词：主站模块、主站、本地站、远程 I/O 站、现场设备站、远程 I/O 网络模式、远程网络模式、循环传送、瞬时传送

CC-Link 是 CLPA（CC-Link 协会）最先推出的、可同时进行控制和信息传递的高速现场总线。传输速率高达 10Mbit/s 时，传输距离为 100m，可支持 64 个站。因其卓越的性能，被授予 SEMI 认证。其开放性也在不断地加速中。此外，还有 CC-Link Safety，是 CC-Link 实现安全系统架构的安全现场网络，与 CC-Link 具有高度的兼容性，可以使用如 CC-Link 电缆或远程站等既有资产和设备。“CC-Link Safety”也能够实现与 CC-Link 一样的高速通信，并提供实现可靠操作的 RAS 功能。

4.2.1 CC-Link 简介

1. CC-Link 组成

CC-Link 可由 1 个主站和多达 64 个从站组成，它采用总线方式连接各个站点。还可通过网关实现从 CC-Link 到 ASI、CC-Link、LT 等网络的连接。

（1）主站

为配置有 CC-Link 主站模块的 PLC 或配置有 CC-Link 接口卡的计算机。主站用以管理网络。一个网络需要 1 个主站，也只能有一个主站。但可以设置备用主站。主站通常需要进行 CC-Link 用网络参数的设定。在安装于主站的主站模块上设定的 CC-Link 用的站号为 0。

网络通信主要由主站管理与发起，从站接收管理与响应。主站可对所有从站进行循环传送（与本地站可进行 $N:N$ 通信），对本地站、现场设备站还可进行瞬时传送（通信）。

备用主站具有主站功能。主站正常工作时它作为本地站（从站的一种）。主站因发生异常导致不能正常工作时，备用主站转为主站。一旦主站工作恢复正常。备用站又作为本地站。

（2）从站

有本地站、现场设备站及远程站（含远程 I/O 站与远程设备站）。

本地站（Local station，L）为配置有 CC-Link 主模块（Q 型机）或 CC-Link 连接模块（对 FX 型机）的 PLC。可与主站及其他本地站进行循环（$n:n$ 链接）通信。前者还可与主站进行瞬时通信。

远程站含远程 I/O 站与远程设备站，只能与主站循环通信。运程 I/O 站（Remote I/O station，RIO）只能传送位数据，只占一个站号。用以连接数字模块等 I/O 设备；远程设备站（Remote Device Station，RD）可传送位及字数据，可连接数字模块、模拟量模块。

现场设备站（Intelligence Device station）既可与主站循环通信，又可与主站瞬时通信。

在 CC-Link 系统中，每个从站的位信息输入、输出点数各 32 点，字信息的输入输出点数各 4 点。如果传输的信息量大、超过上述限制，可增加占有的站数。具体是：本地模块由用户根据与其他站之间的信息交换情况决定对应必要点数的占有站数（1 站～4 站）。远程 I/O 站只占有 1 站。具有特殊功能的远程设备站、现场设备站则根据与其他站交换的信息量决定各模块的占有站数。

这样虽说一个 CC-Link 网络最多可以连接 64 个从站，实际连接的站点数与各个从站占用的逻辑站数有关。具体计算如下：

$$(1\times a)+(2\times b)+(3\times c)+(4\times d)\leqslant 64\text{站}$$

这里，a 为占用 1 个逻辑站的数；b 为占用 2 个逻辑站的数；c 为占用 3 个逻辑站的数；d 为

占用 4 个逻辑站的数。

此外，计算时还要考虑 PLC 具体 CPU 所能管理的 I/O 点数及具体主站模块性能的限制。

（3）电缆、终端电阻及其他附件

电缆为专用三芯的。其中 2 根用以传输信号，一根用以信号屏蔽。建议使用 CC-Link 专用电缆。如果使用 CC-Link 专用电缆之外的其他电缆，将则不能保证 CC-Link 系统的性能。

终端电阻 110Ω、1/2W，是必不可少的。分布在最远处的网络两端。此外，还有中继器、分支器，转换器可根据需要配置，以扩展站点距离或建立分支结构。

2. CC-Link 网络结构

CC-Link 定义的网络结构较简单，仅定义 3 层，即：物理层、数据链路层及应用层。

（1）物理层

沿用 RS-485 标准。但规定的传输介质除了双绞线，还可使用光纤。图 4-2 所示为它根据 RS-485 协议网络接线简图。与 CC-Link/LT 不同的是主站不要求一定安装在网络的首末端。

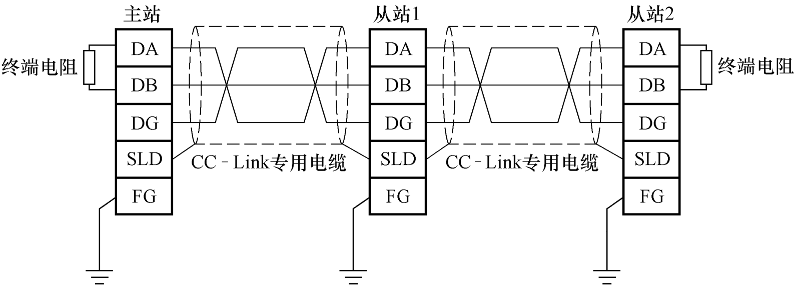


图 4-2　CC-Link 根据 RS-485 协议接线简图

注：连接端子的连接与断开必须在该站电源断开时进行，否则不能保证数据传输。

CC-Link 专用电缆的屏蔽线连接到每一个模块的“SLD”端子上，屏蔽线的两端都通过“FG”与工厂的接地点连接（D 型接地（第 3 种接地））。

SLD 与 FG 应各有独立的接线端子，并应在模块内部连接。

（2）数据链路层

规定的帧格式如图 4-3 所示：



图 4-3　CC-Link 帧格式

这里，F 为一个字节前置码标志段，首尾为 0，中间 6 个位为 1；A1 为发送方地址信息，含义见表 4-1；A2 为接收方地址信息，含义见表 4-1；ST1 为状态信息 1，其各位含义见图 4-4；ST2 为状态信息 2，其各位含义见图 4-5；DATA 为传输实际数据；CRC 为 16 位循环校验码。对从 A1 开始到 DATA 结束之间的数据做计算。

表 4-1　发送方（A1）、接收方（A2）地址信息

A1	A2	描　　述
FFH	n	主站轮询和刷新数据
FEH	n	主站轮询数据
FDH	n	主站测试轮询和测试数据
FCH	n	主站测试轮询数据
FAH	n	刷新循环结束帧
n	FFH	从站响应(刷新)数据(对轮询和刷新数据的响应)
n	FEH	从站响应(刷新)数据(对轮询数据的响应)
n	FDH	从站测试回送数据(对测试轮询和测试数据的响应)
n	FCH	从站测试回送数据(对测试轮询的响应)
n:发送目标(从站站号 1 ~64(1 ~40H),备用主站(80H))		

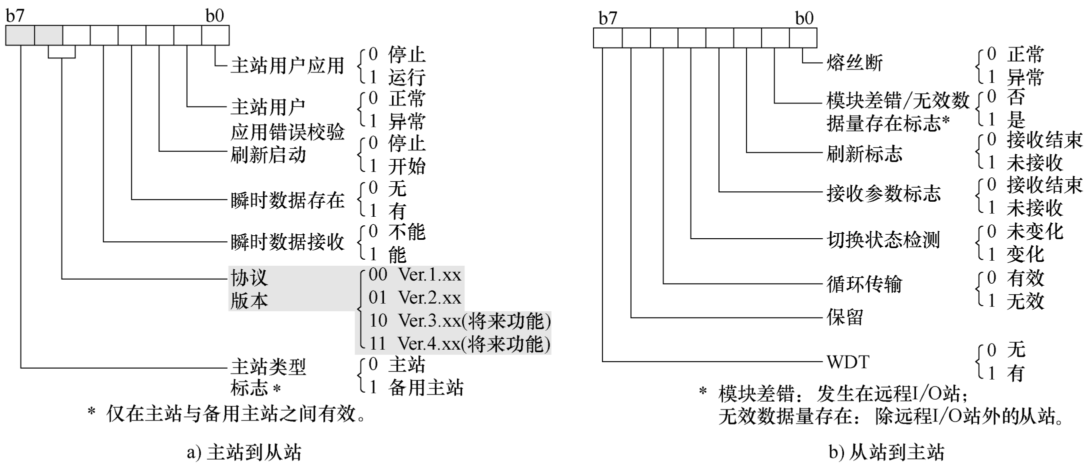


图 4-4　ST1 各位的含义

除了上述还规定：作为发送站，在连续发送 5 个“1”之后要插入一个“0”；作为接收站，在连续收到 5 个“1”之后要的“0”要删除；在刷新循环之间，主站许发送空信号(重复方式为 1010…)；等等。

（3）应用层

规定 CC-Link 为主从网络。通信都是有主站发起，从站响应。规定主站的具体功能有：基本功能，改善系统可靠性的功能，方便功能。只是这些功能与所配置的主站模块及其连接的主机有关。有的可能没有这么多功能。

1）基本功能。有两种通信模式：远程 I/O 网络模式和远程网络模式。而远程网络模式又有这两种模式，即循环传送及瞬时传送。用哪一种可以对主站模块设置确定。

（a）远程 I/O 网络模式。在本模式中，主站仅和远程 I/O 站执行高速循环传送。开关量数据通过远程输入三菱称为输入位的 RX（32 位）和远程输出位的 RY（32 位）传递，可以缩短链接扫描时间，输入输出响应可靠，并且响应时间快，可靠和具有确定性。图 4-6 所示为主站与远程 I/O 站通信概况。

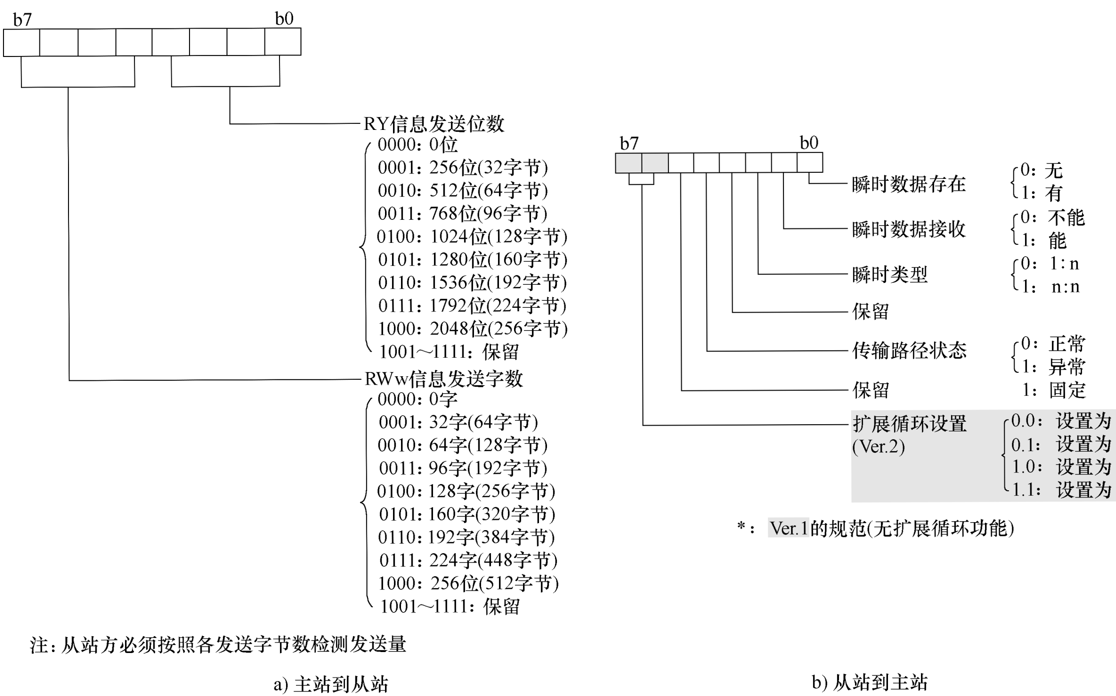


图 4-5　ST2 各位的含义

图 4-6a 所示为数据链接基本过程。

图 4-6b 所示为远程输入的过程。远程 I/O 站的输入状态先自动存储（每次链接扫描时）在主站的“远程输入 RX”缓冲存储器中，然后经 PLC 自动刷新再存储在用参数设定的 PLC 的软元件（X）中。

图 4-6c 所示为远程输出的过程。先是 PLC 自动刷新，把 PLC 软元件（Y）的状态存储在“远程输出 RY”缓冲存储器中。后再经链接扫描，把存储在“远程输出 RY”缓冲存储器中的状态输出到远程 I/O 站。

各小图中的各个标注箭头的含义分别为

a）PLC 系统电源接通时，PLC CPU 中的网络参数传送到主站，CC-Link 系统自动启动。

b）远程 I/O 站的输入状态自动存储（每次链接扫描时）在主站的“远程输入 RX”缓冲存储器中。

c）存储在“远程输入 RX”缓冲存储器中的输入状态存储在用自动刷新参数设定的 CPU 软元件中。

d）用自动刷新参数设置的 CPU 软元件开/关数据存储在“远程输出 RY”缓冲存储器中。

e）存储在“远程输出 RY”缓冲存储器中的输出状态自动输出（每次链接扫描的时候）到远程 I/O 站。

从上述介绍可知，有了这样数据链接过程，PLC 对远程 I/O 的管理其实就可通过对 PLC 软元件 X、Y 的管理实现。这与对当地 I/O 的管理所差的只是连接扫描引起的延迟，而从编程的角度看，两者是感觉不到差别的。

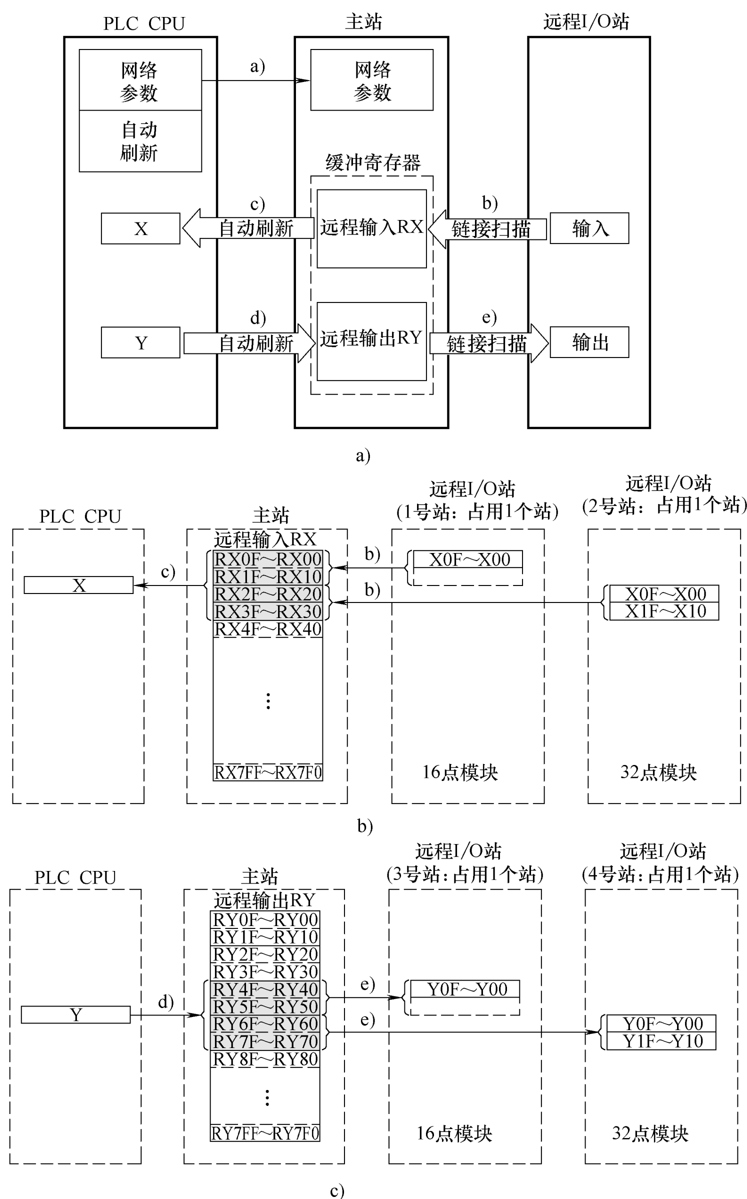


图 4-6 主站与远程 I/O 站通信

（b）远程网络模式循环传送。在本模式中，主站可和所有站（远程 I/O 站、远程设备站、本地站、现场设备站和备用主站）通信。除了传送上述位数据，还要传送字（RWw、RWr，各 4 个字）数据。其机理和主站与远程 I/O 从站通信相同。只是多了使用 RWw 及 EWr 两组远程寄存器。这里不再赘述。

这里要着重介绍的是主站与本地站通信。循环传送是使用远程输入 RX 和远程输出 RY（本地站系统中使用的位数据）以及远程寄存器 RWw 和远程寄存器 RWr（本地站系统中使用的用于读写的字数据）以 N: N 的模式进行。其过程如图 4-7 所示。

图中各个标注箭头的含义分别为

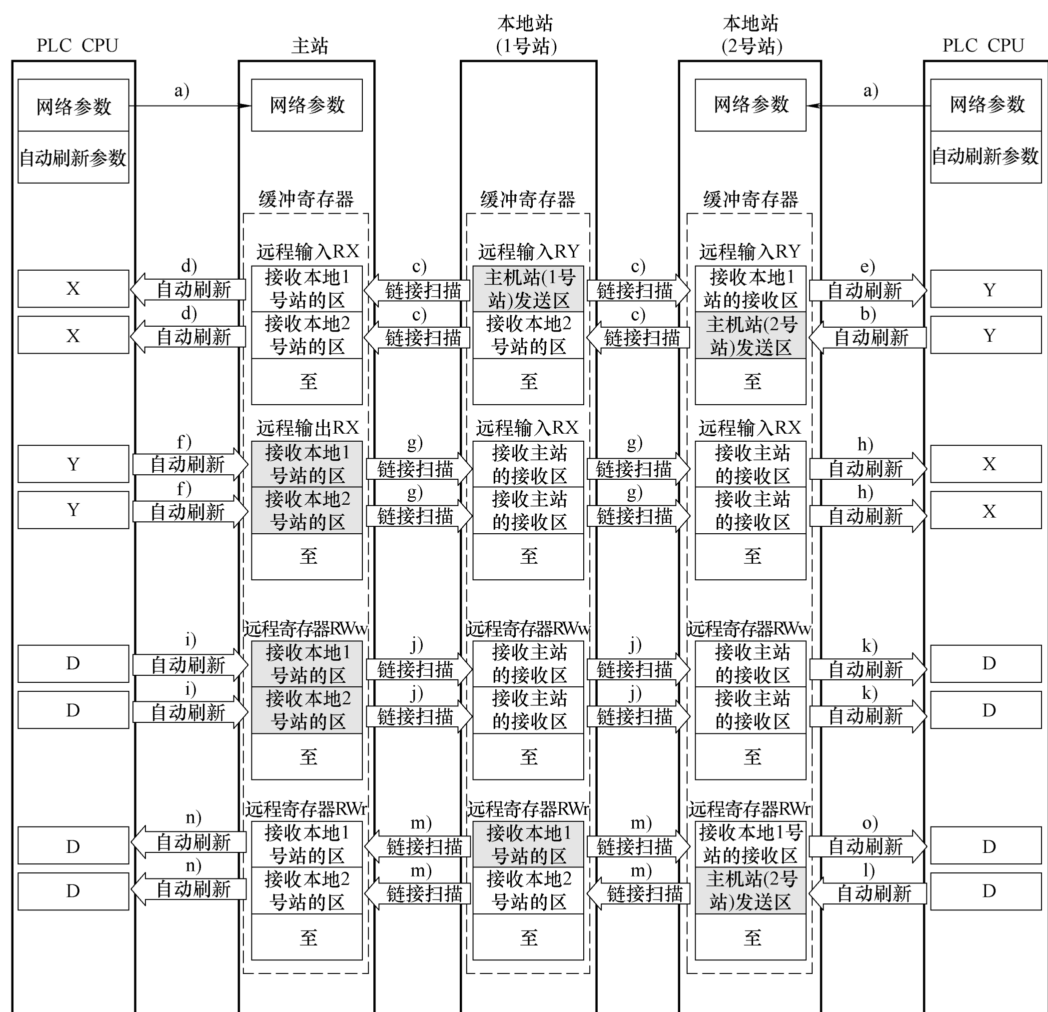


图4-7　远程网络模式循环传送过程

a）PLC系统电源接通时，PLC CPU中的网络参数传送到主站，CC-Link系统自动启动。

b）用自动刷新参数设置的CPU软元件的开/关数据存储在本地站的“远程输出RY”缓冲存储器中。远程输出RY用作在本地站系统中的输出数据。

c）本地站“远程输出RY”缓冲存储器中的数据自动存储（每次链接扫描的时候）在主站的“远程输入RX”缓冲存储器和其他本地站中的“远程输出RY”缓冲存储器中。

d）存储在“远程输入RX”缓冲存储器中的输入状态存储在用自动刷新参数设定的CPU软元件中。远程输入RX用作本地站系统中的输入数据。

e）存储在“远程输出RY”缓冲存储器中的输入状态存储在用自动刷新参数设定的CPU软元件中。

f）用自动刷新参数设置的CPU软元件开/关数据存储在主站的“远程输出RY”缓冲存储器中。

g）在“远程输出RY”缓冲存储器中的数据自动存储（每次链接扫描时）在本地站的

“远程输入 RX”缓冲存储器中。

h）存储在缓冲存储器中的输入状态“远程输入 RX”存储在用自动刷新参数设置的 CPU 软元件中。

i）由自动刷新参数设置的 CPU 软元件字数据存储在主站的“远程寄存器 RWw”缓冲寄存器中。远程寄存器 RWw 用作本地站系统中写的字数据。

j）缓冲存储器“远程寄存器 RWw”中的数据自动存储（每次链接扫描的时候）在所有本地站的缓冲存储器“远程寄存器 RWr”中。远程寄存器 RWr 用作本地站系统中读的字数据。

k）存储在缓冲存储器“远程寄存器 RWr”中的字数据存储到用自动刷新参数设置的 CPU 软元件中。

l）由自动刷新参数设置的字数据存储在本地站的“远程寄存器 RWw”缓冲存储器中。但是，数据仅存储在与其自己的站号相对应的区域。

m）“远程寄存器 RWr”缓冲存储器中的数据自动存储（每次链接扫描的时候）到主站的“远程寄存器 RWr”和其他本地站的“远程寄存器 RWw”中。

n）存储在“远程寄存器 RWr”缓冲存储器中的字数据存储到用自动刷新参数设定的 CPU 软元件中。

o）存储在“远程寄存器 RWw”缓冲存储器中的字数据存储到用自动刷新参数设定的 CPU 软元件中。

有了以上循环传送，实际上 PLC 对远程 I/O 的管理与对当地 I/O 的管理并无本质差别。所差的只是增加循环传送过程的延时。而这个延时是可计算的。如果不满足要求也可起用将要介绍的循时传送。

（c）远程网络模式瞬时传送。在主站与本地站之间还可在任意时刻通过指定另一方以 1∶1的模式进行瞬时传送和接收数据。这时要在主站运行程序，执行相应读（RIRD）、写（RIWT）数据指令（对三菱 Q 型机而言），发起通信，从站响应；主站不执行通信指令，通信停止。

A）使用 RIWT 指令把数据写入本地站中的缓冲存储器的过程如图 4-8 所示。图中各个标注箭头的含义分别为

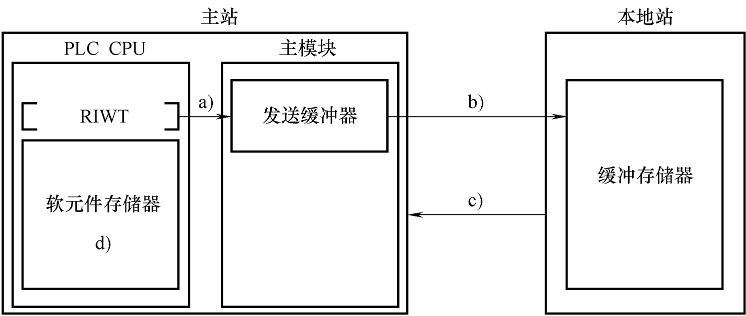


图 4-8　数据写入本地站中的缓冲存储器的过程

a）要写入本地站中的缓冲存储器的数据存储在主站模块的发送缓冲区中。

b）数据写入本地站的缓冲存储器中。

c）本地站向主站回送一个写入完成回应。

d）接通用 RIWT 指定的软元件。

B）使用 RIRD 指令从本地站中的缓冲存储器读取数据的过程如图 4-9 所示各个标注箭头的含义分别为

a）访问本地站缓冲存储器中的数据。

b）读取的数据存储在主站的接收缓冲区中。

c）数据存入 PLC CPU 的软元件存储器中，并接通用 RIRD 指令指定的软元件。

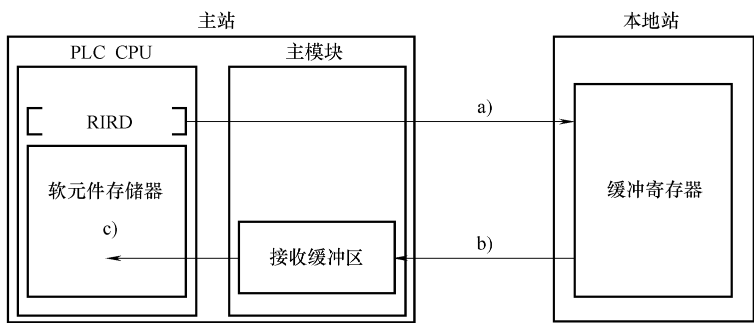


图 4-9　从本地站中的缓冲存储器读取数据的过程

提示：在通过瞬时传送执行数据通信之前，必须在主站的缓冲存储器中把发送和接收缓冲区的大小设定好。

主站除了可与本地站进行循时通信，也可与智能站进行循时通信。表 4-2 所示为三菱 Q 型机主站与现场设备站可使用的通信指令。

表 4-2　三菱 Q 型机主站与现场设备站可使用的通信指令

适用站	指令	说　　明	适用站	指令	说　　明
智能设备站	RIRD	从指定站的缓冲存储器中读取数据	智能设备站	RISEND	和指定站自动交换数据并向这些站的缓冲存储器写入数据
	RIWT	同指定站的缓冲存储器写入数据		RIFR	从指定站的自动更新缓冲区中读取数据
	RIRCV	和指定站自动交换数据并从这些站的缓冲存储器中读取数据		RITO	向指定站的自动更新缓冲区写入数据

2）改善系统可靠性的功能。为确保系统可靠工作，CC-Link 提供很多相关功能。如断开数据链接出错的站并仅在正常站之间进行数据通信（从站断开功能）；出错站恢复正常时自动重新连接已断开的数据链接出错站（自动恢复功能）；主站 PLC CPU 发生错误时继续数据链接（主站 PLC CPU 有错时的数据链接状态设置）；保持数据链接出错站的软元件状态（设定来自数据链接出错站的输入数据的状态）；即使在主站异常时继续数据链接（备用主站功能）；等等。

这几个功能中最重要的是备用主站功能。有了它，即使主站因为 PLC CPU 出故障或断

电引起故障，系统可起用备用主站（即主站的备用站），就会使数据链接继续进行。而且即使在备用主站控制数据链接时，主站也可以恢复到正常模式并作为备用主站恢复到系统运行状态，这样在备用主站宕机的时候，也能接替工作（主站双工功能）。

为此当然要做相应设置。其方法是用编程软件 GPPW，对主站及备用主站做相应设置。

（a）主站设置。首先，设置网络参数中的“类型”。可设置宕机的主站可恢复到系统运行（双工功能）或宕机的主站不恢复到系统运行：然后，设置网络参数中的“备用主站号”。设定范围：1～64（空白意味着不指定备用主站）。缺省：空白（不指定备用主站）。

（b）备用主站设置。将网络参数中的“类型”设置为“备用主站”。将模式设置为“在线（远程网络模式）”。

这些个功能也称 RAS，是 Reliability（可靠性）、Availability（有效性）、Serviceability（可维护性）的缩写，是 CC-Link 的一大特点，说明它可以给用户提供高稳定性的网络，可以最大限度地缩小系统宕机时间。

3）方便功能。为了使用方便 CC-Link 还提供很多相关功能，如简化远程设备站的初始化规程注册（远程设备站初始化规程注册功能）；执行高速处理（为中断程序发布事件功能）；只要打开电源就激活数据链接（自动 CC-Link 启动功能）；编制包括在将来要添加的模块的程序（保留站功能）；给一个运行中的站断电而检测不到出错（出错无效站设置功能）；使链接扫描和顺控扫描同步（扫描同步功能）；更换模块而不会检测到出错（暂时出错无效站设置功能）；检测每个本地站的运行（数据链接停止/重新启动功能）；站号重叠检查功能；等等。

在这些功能中，要提及的是为中断程序发布事件功能及扫描同步功能。

前者是为了能够根据指定的远程输入状况，发布中断信号，使 PLC CPU 执行中断程序。这对有必要加快的响应个别远程输入是很有用的。具体功能的使用是用编程软件设置的，所设置的这类事件可多达 16 个。

后者可选定链接扫描是否要和顺控扫描同步。同步模式，指顺控扫描和链接扫描同时开始。在同步模式中，因为链接扫描和顺控扫描同步，那么顺控扫描用的时间长的话，则链接扫描间隔时间会更长。

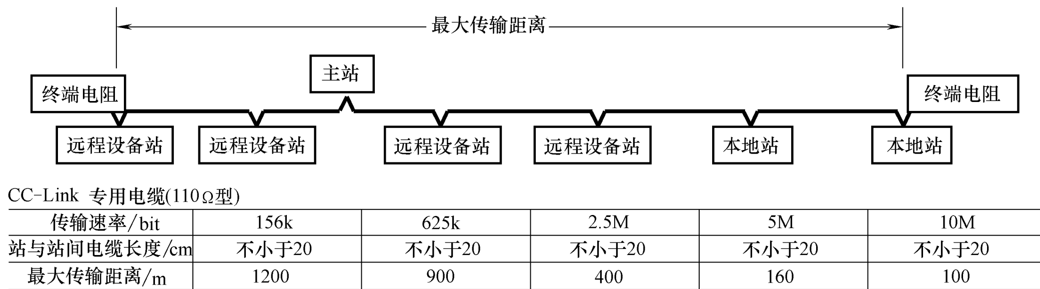
3. CC-Link 拓扑结构

CC-Link 拓扑为总线结构，也允许建立分支。图 4-10 所示为它的总线结构及分支结构的示意。图下小表列出有关传输速度与总线最大距离关系及分支线长度的规定。

CC-Link 还可使用中继器增大网络距离，三菱公司提供这样产品。这使得距离延长可自由自在。因此 CC-Link 可用于大规模的现场，并能够有效较少布线和设备安装的工作量。图 4-11 所示为 CC-Link 在不同传输介质时传输距离与传输速度的关系。

4. CC-Link 性能规格

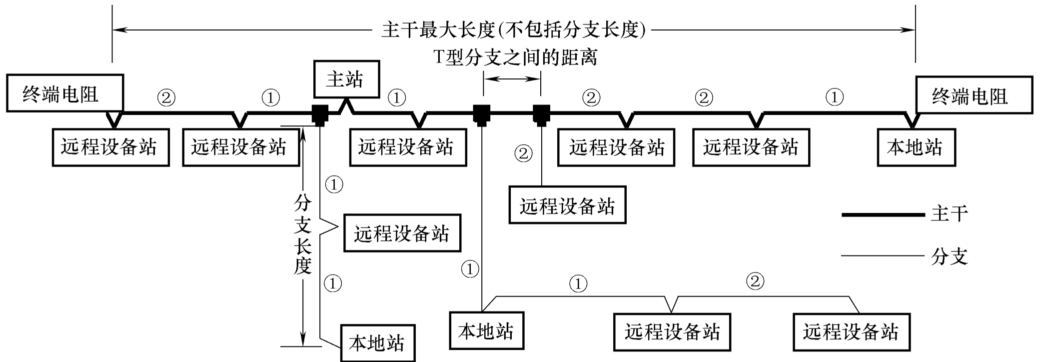
CC-Link 有多个版本，版本高的性能也高，目前最新版本为 2.00。此外还有 Safe（安全）版本，能够及时检出通信延迟、通信数据丢失等通信异常情况，当设备出现故障时，能够实现准确关停。安全远程站的故障和错误信息的历史也能够被保存在安全主站中。这个功能能够更方便进行故障处理。表 4-3 为 2.00 版本的规格。



CC-Link 专用电缆(110Ω型)

传输速率/bit	156k	625k	2.5M	5M	10M
站与站间电缆长度/cm	不小于20	不小于20	不小于20	不小于20	不小于20
最大传输距离/m	1200	900	400	160	100

a) 总线拓扑



项目		描述		备注
传输速率/bit		156k	625k	10M/5M/2.5M不允许带分支
站与站间电缆长度	连接方式1①/m	不小于1		对于仅包含远程I/O站和远程设备站的系统配置
		不小于2		对于包含本地站和智能设备站的系统配置
	连接方式2②/cm	不小于30		
分支连接的最大模块数(每个分支)		6		见通信规范,总连接站数
主干最大长度/m		500	100	终端电阻之间的电缆长度,不包括分支
T型分支之间的距离		无限制		
分支最大长度/m		8		每个分支电缆长度
分支总长度/m		200	50	所有分支的总长度

①:主站与本地站、智能设备站和相邻站之间的距离;
②:远程I/O站与远程设备站之间的距离(最短电缆)。

b) 分支结构

图4-10　CC-Link总线拓扑结构示意

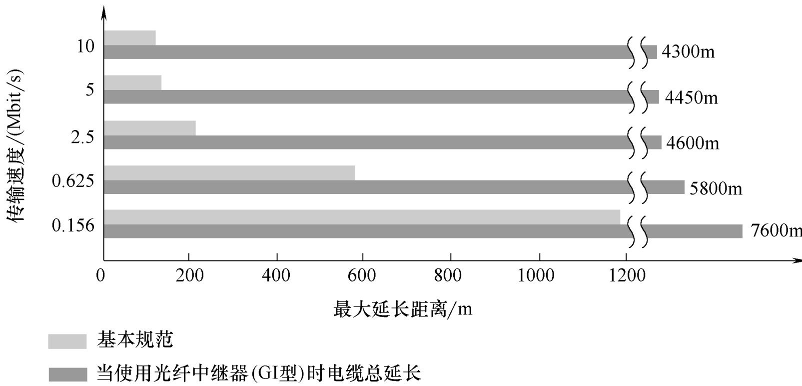


图4-11　CC-Link在不同传输介质时传输距离与传输速度的关系

表 4-3 CC-Link Ver. 2. 00 规格

传输速率/(bit/s)			10M/5M/2. 5M/625k/156k			
最大链接容量	位		8192 (重叠混合时:16384)			
	字		4096 {RWw:2048、RWr:2048}			
扩展循环设置			设置为 1 倍*	设置为 2 倍	设置为 4 倍	设置为 8 倍
每站的链接容量	—	位	32 {重叠混合时 64}	32 {重叠混合时 64}	64 {重叠混合时 128}	128 {重叠混合时 256}
		字	8 {RWw:4、RWr:4}	16 {RWw:8、RWr:8}	32 {RWw:16、RWr:16}	64 {RWw:32、RWr:32}
每个占用内存站的链接容量	占用 1 内存站	位	32 {重叠混合时 64}	32 {重叠混合时 64}	64 {重叠混合时 128}	128 {重叠混合时 256}
		字	8 {RWw:4、RWr:4}	16 {RWw:8、RWr:8}	32 {RWw:16、RWr:16}	64 {RWw:32、RWr:32}
	占用 2 内存站	位	64 {重叠混合时 128}	96 {重叠混合时 192}	192 {重叠混合时 384}	384 {重叠混合时 768}
		字	16 {RWw:8、RWr:8}	32 {RWw:16、RWr:16}	64 {RWw:32、RWr:32}	128 {RWw:64、RWr:64}
	占用 3 内存站	位	96 {重叠混合时 192}	160 {重叠混合时 320}	320 {重叠混合时 640}	640 {重叠混合时 1280}
		字	24 {RWw:12、RWr:12}	48 {RWw:24、RWr:24}	96 {RWw:48、RWr:48}	192 {RWw:96、RWr:96}
	占用 4 内存站	位	128 {重叠混合时 256}	224 {重叠混合时 448}	448 {重叠混合时 896}	896 {重叠混合时 1792}
		字	32 {RWw:16、RWr:16}	64 {RWw:32、RWr:32}	128 {RWw:64、RWr:64}	256 {RWw:128、RWr:128}
占用站数(本地站时)			4 站			
瞬时传输 (每个链接扫描)			最多 960 字节/内存站 【150 字节(主站→智能设备站或本地站)34 字节(智能设备站或本地站→主站)】			
连接模块数			①(a + a2 + a4 + a8) + (b + b2 + b4 + b8) × 2 + (c + c2 + c4 + c8) × 3 + (d + d2 + d4 + d8) × 4 ≤ 64(内存站) ②(a × 32 + a2 × 32 + a4 × 64 + a8 × 128) + (b × 64 + b2 × 96 + b4 × 192 + b8 × 384) + (c × 96 + c2 × 160 + c4 × 320 + c8 × 640) + (d × 128 + d2 × 224 + d4 × 448 + d8 × 896) ≤ 8192(位) ③(a × 4 + a2 × 8 + a4 × 16 + a8 × 32) + (b × 8 + b2 × 16 + b4 × 32 + b8 × 64) + (c × 12 + c2 × 24 + c4 × 48 − c8 × 96) + (d × 16 + d2 × 32 + d4 × 64 + d8 × 128) ≤ 2048(字) a:占用 1 内存站设置为 1 倍模块数　b:占用 2 内存站设置为 1 倍模块数 c:占用 3 内存站设置为 1 倍模块数　d:占用 4 内存站设置为 1 倍模块数 a2:占用 1 内存站设置为 2 倍模块数　b2:占用 2 内存站设置为 2 倍模块数 c2:占用 3 内存站设置为 2 倍模块数　d2:占用 4 内存站设置为 2 倍模块数 a4:占用 1 内存站设置为 4 倍模块数　b4:占用 2 内存站设置为 4 倍模块数 c4:占用 3 内存站设置为 4 倍模块数　d4:占用 4 内存站设置为 4 倍模块数 a8:占用 1 内存站设置为 8 倍模块数　b8:占用 2 内存站设置为 8 倍模块数 c8:占用 3 内存站设置为 8 倍模块数　d8:占用 4 内存站设置为 8 倍模块数 ④16 × A + 54 × B + 88 × C ≤ 2304 A:远程 I/O 站模块数 ………………………… 最多 64 台 B:智能设备站模块数 ………………………… 最多 42 台 C:本地站、智能设备站模块数 ………………………… 最多 26 台			
输入输出占用点数			32 点(I/O 分配:智能 32 点)			

从所示规格可知，CC-Link 可实现高速大容量的数据传输。每个内存站循环传送数据为 24 字节，其中 8 字节（64 位）用于位数据传送，16 字节（ 4 点 RWr 、4 点 RWw）用于字

传送。一个物理站最大占用 4 个内存站，故一个物理站的循环传送数据为 96 个字节。在循环传输数据量不够用的情况下，CC-Link 提供瞬时传输功能，可将 960 字节的数据，用指令传送给目标站。CC-Link 在连接 64 个远程 I/O 站、通信速度为 10Mbit/s 的情况下，循环通信的链接扫描时间为 3.7ms。稳定快速的通信速度是 CC-Link 的最大优势。

4.2.2　三菱 CC-Link 组件

三菱是 CC-Link 创始者，目前它的 CC-Link 产品也最为齐全。以下对它的主要 CC-Link 产品做简要介绍。

1. 主站模块

1）QJ61BT11 主站模块。可作为智能模块安装在 Q 型机任意基板的 I/O 槽上，以使 PLC 作为 CC-Link 的主站。也可使 PLC 作为 CC-Link 的备用主站或本地站。具体由对模块的设置确定。图 4-12 所示为它的面板外观。其中 1 为指示灯，2 为站号设定开关，3 为模式设定开关，4 为接线端口。表 4-4 所示为它的几个指示灯含义。

表 4-4　QJ61BT11 主站模块几个指示灯含义

LED 名称	说　　明
RUN	On:模块正常运行时 Off:警戒定时器出错时
ERR.	On:所有站有通信错误 发生下列错误时也会亮起 ● 开关类型设置不对 ● 在同一条线上有一个以上的主站 ● 参数内容中有一个错误 ● 激活了数据链接监视定时器 ● 断开电缆连接 或者传送路径受到噪声影响 如何检查错误来源 和 SW0058 有关的细节(LED 显示器状态详述)请参考其他资料 闪烁:某个站有通信错误
MST	On:作为主站运行(数据链接控制期间)
S MST	On:作为备用主站运行(备用期间)
L RUN	On:正在进行数据链接
L ERR.	On:通信错误(上位机) 以固定时间间隔闪烁:通电时改变开关 2 和 3 的设置。 以不固定的时间间隔闪烁:没有装终端电阻:模块和 CC-Link 专用电缆受到噪声影响
SD	On:正在进行数据发送
RD	On:正在进行数据接收

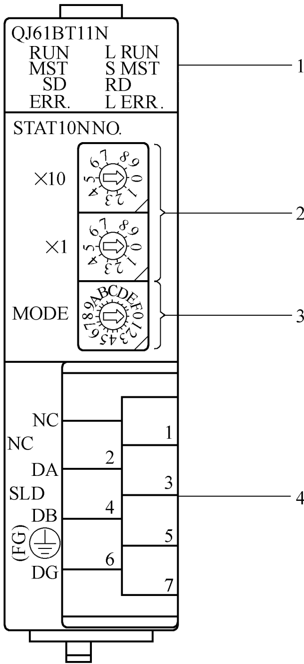


图 4-12　QJ61BT11 主站模块面板外观

作为智能模块安装在 PLC 机架后也要占用 2 个输入、输出字的 I/O 地址的，其占用地址与其他智能模块一样，由安装它的位置和安装它前面的模块决定。这 4 个字中输出字被禁止使用，输入字的多数位用户也不能用，只有模块出错位（Xn0，表示模块是正常还是异常，OFF：模块正常；ON：模块出错）、上位机数据链接状态位（Xn1，说明上位站的链接状态，OFF：数据链接停止；ON：数据链接正在进行）、模块准备好位（XnF，说明模块是

否准备好运行，模块进入准备好运行状态时：ON；检测到模块开关设置状态出错或模块出错信号 Xn0 ON：OFF，等若干位可用以监视网络状态。这里 n 指的是模块首位所在字地址。

存储与从站通信的数据以及和 PLC CPU 之间传送数据主站模块数据更主要是用容量有 20k 之大的主站模块缓冲存储器（BFM）。同时，它也是用于 CC-Link 系统的工作区。上已提及的远程输入 RX、远程输出 RY 及远程寄存器 RWr、RWw 就是这缓冲存储器的一部分。表 4-5 所示为这个缓冲存储器的与用户相关部分的明细。

表 4-5　主站模块缓冲存储器部分明细

地址		项　　目	说　　明	读/写可能性	可用性	
十六进制	十进制				主站	本地站
$E0_H$ ~ $15F_H$	224 ~ 351	远程输入(RX)	用于主站:存储来自远程站/本地站/智能设备站/备用主站的输入状态	只读	○	—
			用于本地站:存储来自主站的输入状态		—	○
160_H ~ $1DF_H$	352 ~ 479	远程输出(RY)	用于主站:存储要发到远程站/本地站/智能设备站/备用主站的输出状态	只写	○	—
			用于本地站:存储要发到主站的输出状态。同时存储收到的来自远程站/其他本地站/智能设备站/备用主站的数据	允许读/写	—	○
$1E0_H$ $2DF_H$	480 ~ 735	远程寄存器(RWw) 主站:用于发送 本地站:用于发送和接收	用于主站:存储发到远程设备站/所有本地站/智能设备站/备用主站的数据	只写	○	—
			用于本地站:存储发到远程主站/其他本地站/智能设备站/备用主站的数据。同时存储来自远程设备站/其他本地站/智能设备站/备用主站的数据	允许读/写	—	○
$2E0_H$ ~ $3DF_H$	736 ~ 991	远程寄存器(RWr) 主站:用于接收 本地站:用于接收	用于主站:存储接收的来自远程设备站/本地站/智能设备站/备用主站的数据	只读	○	—
			用于本地站:存储接收的来自主站的数据		—	○
$5E0_H$ ~ $5FF_H$	1504 ~ 1535	链接特殊继电器(SB)	存储数据链接状态	允许读/写（根据设备的不同,可能禁止写入）	○	○
600_H ~ $7FF_H$	1536 ~ 2047	链接特殊寄存器(SW)	存储数据链接状态		—	—
$A00_H$ ~ FFF_H	2560 ~ 4095	随机访问缓冲区	瞬时传送时存储和使用指定的数据	允许读/写	○	○
1000_H ~ $1FFF_H$	4096 ~ 8191	通信缓冲区	和本地站、备用主站和智能设备站进行瞬时传送时(用通信缓冲区通信)存储发送和接收的数据以及控制数据	允许读/写	○	○
2000_H ~ $2FFF_H$	8192 ~ 12287	自动更新缓冲区	和 AJ65BT-R2 进行瞬时传送时(用自动更新缓冲区通信)存储自动更新数据	允许读/写	○	○

注：○：可用，—：不可用。

表中的缓冲存储器中链接特殊继电器（SB）用位 ON/OFF 数据存储数据链接状态；链接特殊寄存器（SW）用字数据存储数据链接状态；随机访问缓冲区存储要发送到其他站的任何数据，瞬时传送时要用到这个区。通信缓冲区在进行本地站、备用主站和现场设备站之间的瞬时传送时要用到它（使用 RIRD、RIWT、RIRCV 及 RISEND 指令）。自动更新缓冲区存储自动更新数据，进行如 AJ65BT-R2 RS-232C 串口这样现场设备站进行瞬时传送要用到它（使用 RIFR、RITO 指令）。循时传送选用的缓冲区依从站而异。在使用之前其大小也要先做设置，要比将要传送的数据略大。

对缓冲存储器的详细了解，特别对链接特殊继电器及链接特殊寄存器的了解，对做好网络设置及有关编程是很有必要的。缓冲存储器的使用具体说明可参阅该模块的说明书。

缓冲存储器可用编程软件 GX Developer 通过参数设置或专用的 FROM、TO 指令进行读写。但电源关闭或者复位 PLC CPU 时缓冲存储器的内容恢复到缺省值。不过可使用 EEROM 记录这设定值，待 PLC 重新上电时又可恢复为设定值。

2）FX2N-16CCL-M 主站模块。为小型机用的主站模块，可作为智能模块与 FX、F3UC 型机连接，以使 PLC 作为 CC-Link 的主站。使用 FX2N-16CCL-M 主站模块组成 CC-Link 网络受小型性能限制功能要少些。不能进行循时传送，连接的站点数及可控制的 I/O 点数也要少些。即使新推出的 FX3U 机可控制的当地输入输出点数加 CC-Link 远程 I/O 点数也不能超过 384 点。

它作为智能模块与 PLC 相连也要占用 1 个输入或输出 I/O 地址，其占用地址与其他智能模块一样，由安装它前面的模块决定。只是这个字被禁止使用。

存储与从站通信的数据以及和 PLC CPU 之间传送数据主站模块数据更主要是用主站模块缓冲存储器（BFM）。同时，它也是用于 CC-Link 系统的工作区。只是它的这个较小，仅 2KB。它的 RX 在缓冲存储器中的地址为 E0H 到 FDH；RY 在缓冲存储器中的地址为 160H ~ 17DH；RWr 在缓冲存储器中的地址为 2E0H ~ 31BH；RWw 在缓冲存储器中的地址为480H ~ 539H；链接特殊继电器 SB 在缓冲存储器中的地址为 5E0H ~ 5FFH；链接特殊寄存器 SW 在缓冲存储器中的地址为 600H ~ 7FFH。

再就是它的缓冲存储器不能用编程软件 GX Developer 做参数设置，智能用 FROM、TO 指令进行读写。这也是它的功能不如 Q 型机之处。

3）用于安装在计算机上主站接口板，如 ECP-CL2BD、Q80BD-J61BT11N 等。将其安装在计算机的 PCI 槽上，可使计算机成为 CC-Link 的主站、备用站或本地站。同时，三菱还提供有相应的使用软件。只是它多只用于网络的监测、设置，实际用处不大。

4）此外，还提供可连接 CC-Link/lT、AS-i 网络的网桥模块。可用其做 CC-Link 的从站，做后者的主站，使后者的从站也接入 CC-Link 网络。

2. 从站模块

从站模块类型、规格很多，有：远程 I/O 模块、小型远程 I/O 模块、模拟数字转换模块、数字模拟转换模块、高速计数模块、温度输入模块、图形操作模块、RS-232 接口模块，等等。这些模块有的可作为 CC-Link 的远程 I/O 站，有的可作为 CC-Link 的远程设备站，有的可作为 CC-Link 的远程智能站。表 4-6 为其部分模块一览表。

表 4-6　三菱 CC-Link 部分从站模块一览表

产品名称	型号名称	说　　明	占用的站数	站类型
远程 I/O 模块	AJ65BTB1-16D	单线直流输入 16 点模块(漏/源共享) 24V 直流,7mA,16 点/公共	一个站	远程 I/O 站
	AJ65BTB1-16DT	I/O 模块 输入:单线直流输入 8 点(漏) 24V 直流,7mA,8 点/公共 输出:单线晶体管输出 8 点(漏) 12/24V 直流,0.5A/点,4A/公共,8 点/公共		
	AJ65SBTB1-16T	单线晶体管输出 16 点模块(漏) 12/24V 直流,0.5A/点,3.6A/公共,16 点/公共 …		
	AJ65BTB2-16DR	I/O 模块 输入:双线直流输入 8 点(漏/源共享) 24V 直流:7mA,8 点/公共 输出:双线触点输出 8 点 24V 直流/240V 交流,2A/点,8A/公共,8 点/公共		
小型远程 I/O 模块	AJ65SBTB1-8D	单线直流输入 8 点模块(漏/源共享) 24V 直流,7mA,8 点/公共 …	1 个站	
	AJ65SBTC4-16DT	I/O 模块 输入:2、3、4 线直流输入 8 点(漏) 24V 直流,5mA,16 点/公共 输出:2、3、4 线晶体管输出 8 点(漏) 24V 直流,0.5A/点,16 点/公共		
	AJ65SBTW4-16DT	I/O 模块,防水型 输入:防水,4 线直流输入 8 点(漏) 24V 直流,5mA,16 点/公共 输出:防水,4 线晶体管输出 8 点(漏) 24V 直流,0.5A/点,16 点/公共		
模拟—数字转换模块	AJ65BT-64AD	4 通道输入 模拟输入:-10 ~ +10V、-20 ~20mA 数字输出:-2000 ~ +2000,0 ~ +4000	2 个站	远程设备站
数字—模拟转换模块	AJ65BT-64DAV	4 通道电压输出 数字输入:-2000 ~ +2000 模拟输出:-10 ~ +10V		
	AJ65BT-64DAI	4 通道电流输出 数字输入:0 ~ +4000 模拟输出:4 ~20mA		
高速计数模块	AJ65BT-D62	24 位二进制,5/12/24V 直流输入型 200k 脉冲/s,2 通道	4 个站	
	AJ65BT-D62D	24 位二进制,5/12/24V 直流输入型 400k 脉冲/s,2 通道		
	AJ65BT-D62D-S1	24 位二进制,微分型 400k 脉冲/s,2 通道		
热电偶温度输入模块	AJ65BT-68TD	用于连接热电偶 温度输入 8 通道	4 个站	
铂温度测量电阻 Pt100 温度输入模块	AJ65BT-64RD3	用于连接 Pt100(3 线型) 温度输入 4 通道		
	AJ65BT-64RD4	用于连接 Pt100(4 线型) 温度输入 4 通道		

（续）

产品名称	型 号 名 称	说　明	占用的站数	站类型
ID 接口模块	AJ65BT-D32ID2	可以连接的阅读器/写入器的数目是2	4 个站	远程设备站
图形操作终端	A852GOT-LWD/LBD	单色液晶型(2 种颜色) 分辨率:320×240 点 触摸键的数量:300	2 个或4 个站	
	A852GOT-SWD/SBD	STN 彩色液晶型(8 种颜色) 分辨率:320×240 点 触摸键的数量:300		
用于 CC-Link 链接的通信模块	A8GT-J61BT15	用于 GOT 的 CC-Link I/F 模块(用于远程设备站)		
PC 接口板	A80BD-J61BT13	用于 DOS/V PC 的 CC-Link 接口板(用于 PCI 路线插槽)	1 个或4 个站	本地站
RS-232C 接口模块	AJ65BT-R2	计算机链接功能 RS-232C,单通道	1 个站	智能设备站
定位模块	AJ65BT-D75P2-S3	用于定位控制,脉冲链式输出 两个轴(独立,同步双轴,双轴线性插补,双轴弧插补)	4 个站	
用于 CC-Link 连接的通信模块	A8GT-J61BT13	用于 GOT 的 CC-Link I/F 模块 (用于智能设备站)	1 个或4 个站	
用于 GPP 功能的外设连接模块	AJ65BT-G4-S3	用于 GPP 功能的外设连接 RS-422,单通道	1 个站	

此外，还有 FX2N-16CCL 为 FX 机用的本地模块。它可作为智能模块与 FX、F3UC 型机连接，以使 FX 机作为 CC-Link 的本地站。而作为智能模块安装在 Q 型机任意基板的 I/O 槽上的 QJ61BT11 主站模块，通过设定，也可使 PLC 作为 CC-Link 的本地站。本地站实际也是 CC-Link 重要的一种从站。可进行 PLC 之间的链接通信，实现多 PLC 的协调控制。

再就是三菱还提供一些网桥模块，如 CC-Link 与 CC-Link/LT 网桥、CC-Link 到 AS-i 网桥模块。这些模块既是 CC-Link 的从站，又是 CC-Link/LT、AS-i 的主站。可用以把 CC-Link/LT、AS-i 从站模块也接入 CC-Link，使 PLC 可更方便地进行分散的 I/O 控制。

3. 附件

三菱提供有多种中继器：一种为 T 型分支中继器 AJ65SBT-RPT ，每增加一个距离延长一倍。一个网络最多可以使用 10 个。第二种为光中继器 AJ65SBT-RPS 或 AJ65SBT-RPG ，用光缆延长，在一些比较容易受干扰的环境用它较合适。光中继器要成对使用，每一对 AJ65SBT-RPS 之间的延长距离为 1km，最多可以使用 4 对；每一对 AJ65SBT-RPG 之间的延长距离为 2km，最多可以使用 2 对。第三种为空间光中继器 AJ65BT-RPI-10A/AJ65BT-RPI-10B，采用红外线无线传输的方式，在布线不方便，或者连接设备位置会移动的场合使用。空间光中继器也必须成对使用，两者之间的距离不能超过 200m。

4.2.3　三菱 CC-Link 配置实例

1. 主站与远程 I/O 站相连之一

（1） 系统配置

图 4-13 所示为本例系统配置。

从图知，本例主站为 Q 型机，有 3 个远程 I/O 从站，分别是 1、2、3 号站。1 号站是 16

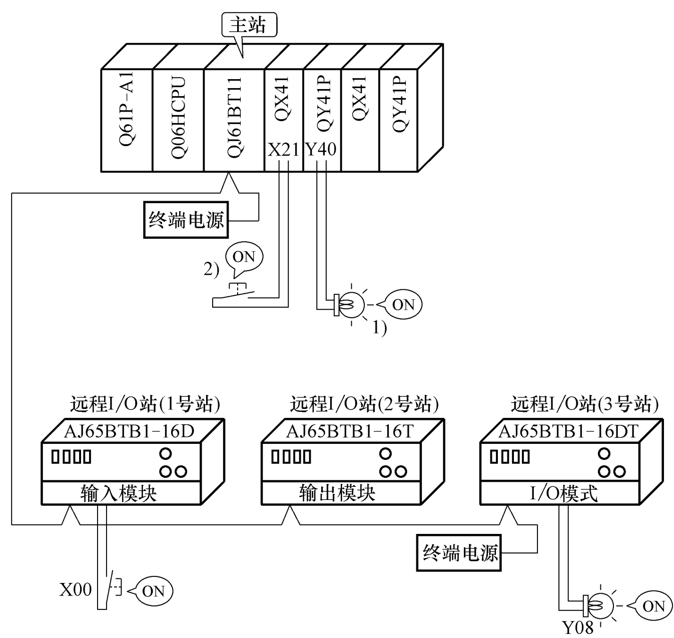


图 4-13　主站与远程 I/O 站相连系统配置例

点输入模块，2 号站是 16 点输出模块，3 号站是 8 点输入、8 点输出混合模块。

要求系统工作后能实现如下要求：当在从站 1 的 X00 ON，则主站的 Y40 ON，否则主站 Y40 OFF；当在主站的 X21 ON，则从站 3 的 Y0B ON，否则从站 3 的 Y0B OFF。当然如果有其他要求，也可用相应程序实现了。

（2）系统设置

对主站、从站都要进行设置。

1）主站硬件设置。要在主站模块的面板上设置站号、模式、传输速率及条件。站号设置开关 0（十位）、0（个位），即主站设为“00”。传送速率/模式设置开关设为 0，即速率 156kbit/s，模式在线。

此外还要用编程软件做网络参数设置。为此，先点击网络参数项 1。之后弹出网络参数小窗口 2。再点击其上“CC-Link”项，将弹出设置窗口 3。有了此窗口即可进行相应设置。图 4-14 所示为本例网络参数设置。

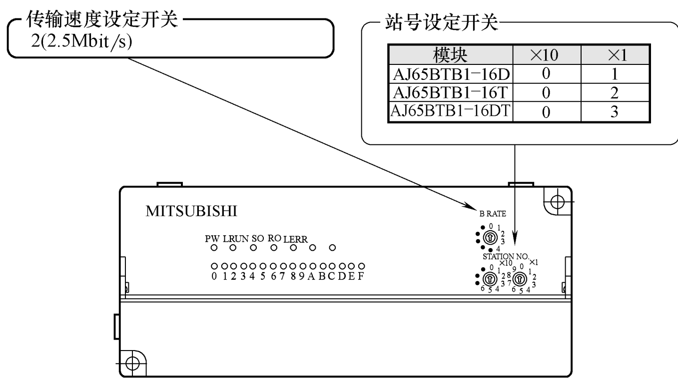
本例设置为 3 个从站，远程 I/O 网络模式，远程输入 RX 对应（刷新）的 PLC 软元件为 X1000（可从 X，M，L，B，D，W，R 或 ZR 中选择），远程输出 RY 对应（刷新）的 PLC 软元件为 Y1000（可从 Y，M，L，B，T，C，ST，D，W，R 或 ZR 中选择），特殊继电器 SB 对应（刷新）的 PLC 软元件为 SB0（可从 M，L，B，D，W，R，SB 或 ZR 中选择），特殊继电器 SW 对应（刷新）的 PLC 软元件为 SW0（可从 M，L，B，D，W，R，SB 或 ZR 中选择），等等。

2）从站设置。要在主站模块的面板上设置站号、传输速率，如图 4-15 所示。

3）经上述设定，PLC CPU 的软元件和远程 I/O 站的输入/输出之间的关系如图 4-16 所示。图中阴影部分表示实际应用的软元件。有了这个对应关系，有关控制程序就可以设计了。



图 4-14　主站网络参数设置例



模块	×10	×1
AJ65BTB1-16D	0	1
AJ65BTB1-16T	0	2
AJ65BTB1-16DT	0	3

图 4-15　从站设置

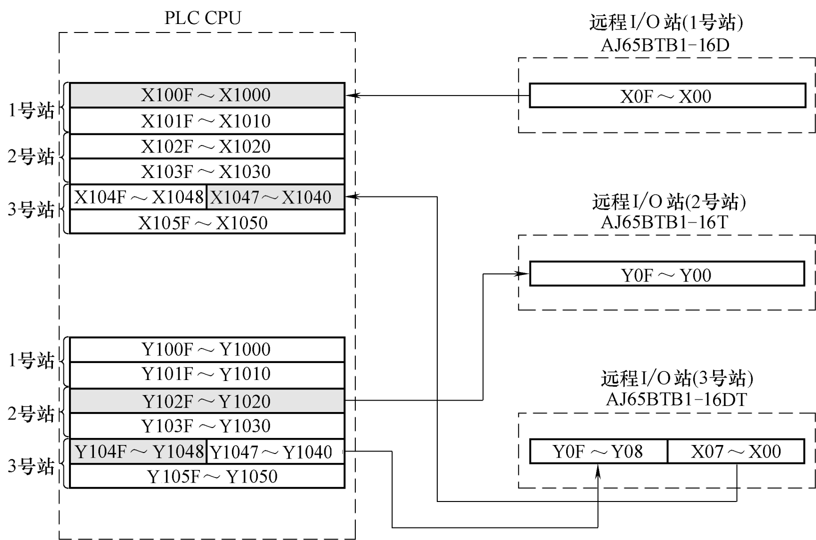


图 4-16　PLC CPU 的软元件和远程 I/O 站的输入/输出之间关系

4）创建程序。有了图 4-16 关系，就可按启动循环通信、实现数据链接及执行读取缓冲存储器及实现用户对控制的要求编写程序。图 4-17 所示为相应控制程序。

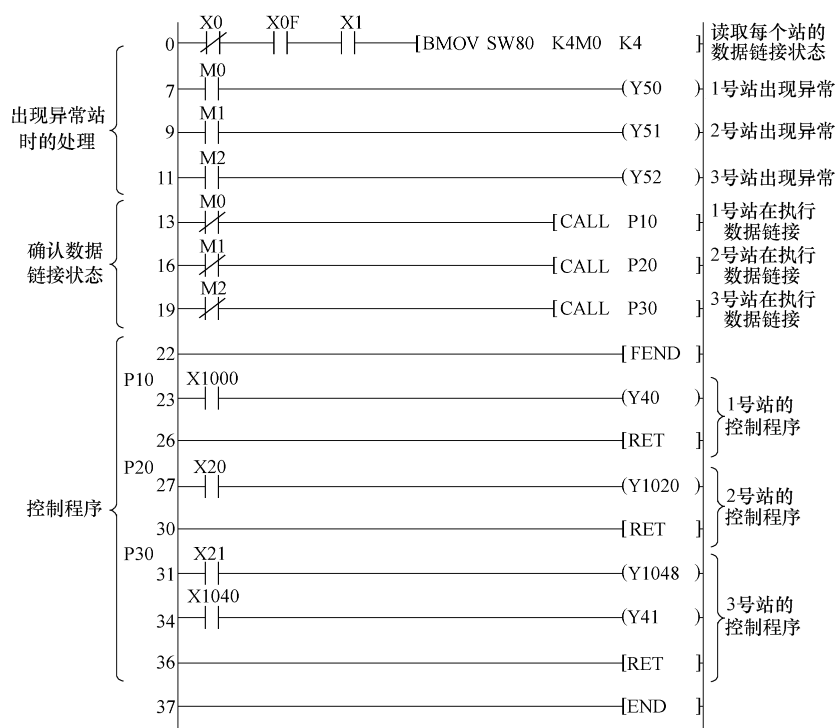


图 4-17 控制程序

5）执行数据链接。首先接通远程 I/O 站的电源，然后接通主站的电源，启动数据链接。之后可用 LED 显示器确认运行情况。图说明了当正常执行数据链接时，主站和远程 I/O 站的 LED 显示状态。

图 4-18 所示主站 LED 的显示。真是如图那样显示，可确认网络工作正常。

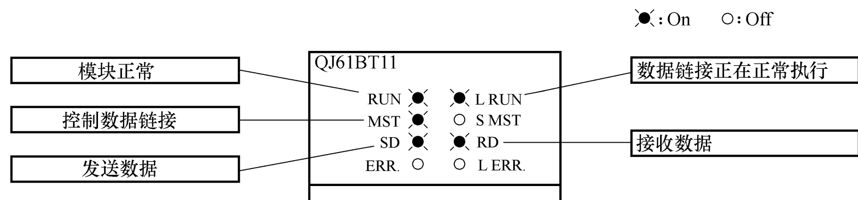


图 4-18 主站 LED 的显示

图 4-19 所示从站 1LED 的显示。真是如图那样显示，可确认从站 1 工作正常。

也可用顺控程序，确认数据链接正在正常执行。例如，当远程 I/O 站 AJ65BTB1-16D（1 号站）的 X00 接通时，主站的 Y40（QY41P）接通，当主站的 X21（QX41）接通时，远程 I/O 站 AJ65BTB1-16DT（3 号站）的 Y08 接通，就可说明链接正常。

2. 主站与远程 I/O 站相连之二

（1）系统配置

图 4-19　从站 1LED 的显示

图 4-20 所示为本例系统配置。

从图知，本例只是主站用 FX 型机，从站与上例相同。

要求系统工作后能实现如下要求：当在从站 1 的 X00 ON，则主站的 Y000 ON，否则主站 Y000 OFF；当在主站的 X000 ON，则从站 2 的 Y00 ON，否则主站 Y00 OFF。当然如果有其他要求，也可用相应程序实现了。

图 4-20　主站与远程 I/O 站相连系统配置例

（2）系统设置

对主站、从站都要进行设置。

1）主站设置。要在主站模块的面板上设置站号、模式、传输速率及条件，如图 4-21 所示。

SW	设定	描述
1	OFF	—
2	OFF	—
3	OFF	—
4	OFF	清除
5	OFF	—
6	OFF	—
7	OFF	—
8	OFF	—

图 4-21　主站设置

此外，还要进行主站网络参数设置。但是，FX 机无法利用编程软件设置，所以，要编写设置程序。

2）从站设置。要在主站模块的面板上设置站号、传输速率，设置同本小节 1. 主站与远程 I/O 站相连一致。

3）主站缓冲存储器与从站链接关系。有了主站与从站的上述设置，起动链接后主站缓冲存储器与从站对应关系如图 4-22 所示。

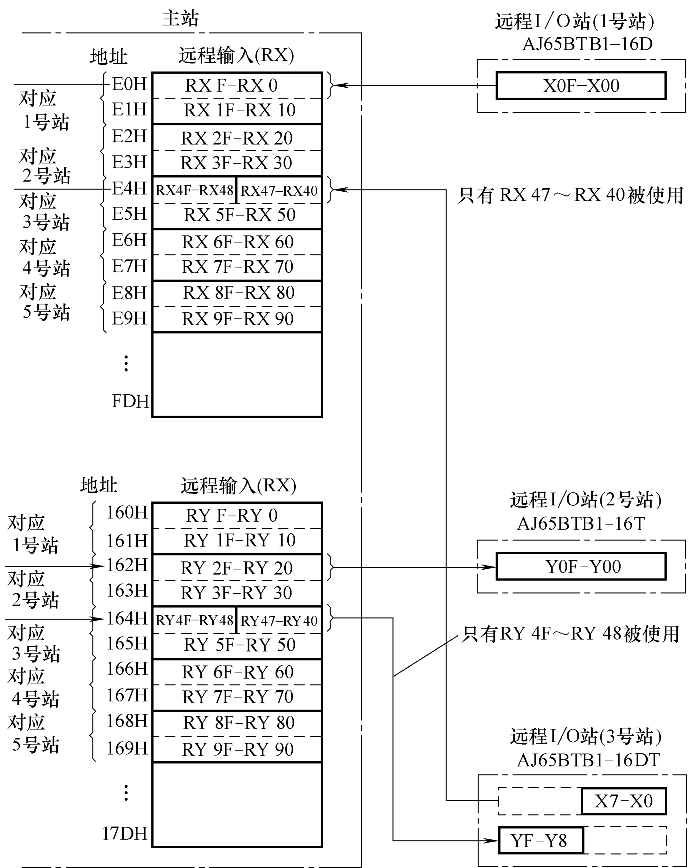


图 4-22 主站缓冲存储器与从站对应关系

4）创建程序。因为主站 PLC 要用程序读写主站模块缓冲存储器的数据，所以所取创建的程序稍复杂些。其编写流程如图 4-23 所示。

图 4-24 所示为用于运行程序。程序已有加注，可对照参数设置阅读。

5）效果检查。可通过指示灯检查，也可通过要求操作及其后果检查。具体略。

3. 主站与本地站相连

（1）系统配置

图 4-25 所示为本例系统配置。系统要求之一是，当主站的 X20 ON 时，本地站的 Y41 ON，否则 Y41 OFF；当本地站的 X21 ON 时，主站的 Y40 ON，否则主站的 Y40 OFF。

（2）系统设置

1）主站设置。主站硬件设置站号为 0（主站），传输速率为 156kbit/s；从站硬件设置站号为 1，传输速率为 156kbit/s、在线。

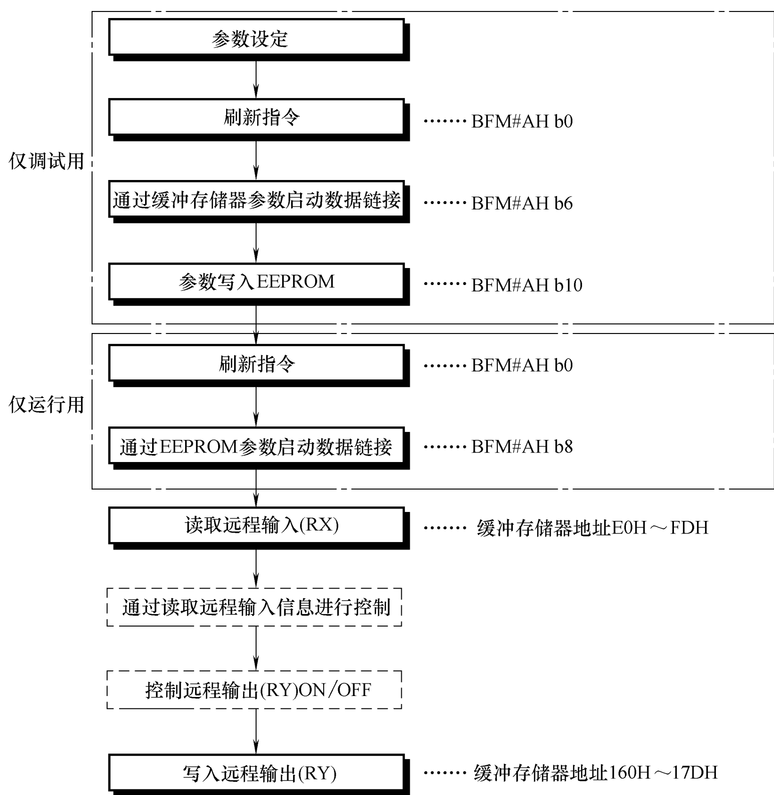


图4-23 程序编写流程

设置主站的网络参数使用编程软件，其方法同本小节介绍的主站与远程站配置实例。主要是：类型：主站，模式：在线远程网络模式、扫描模式：异步，等等。设置主站的自动刷新参数为：将远程输入（RX）的刷新软元件设置为X1000；将远程输出（RY）的刷新软元件设置为Y1000；将远程寄存器（RWr）的刷新软元件设置为D1000；将远程寄存器（RWw）的刷新软元件设置为D2000；将特殊继电器（SB）的刷新软元件设置为SB0；将特殊寄存器（SW）的刷新软元件设置为SW0。

2）本地站设置。网络参数也使用编程软件，其方法也同本小节介绍的主站与远程站配置实例。主要是：类型：本地站，模式：在线远程网络模式，等等。设置本地站的自动刷新参数为：将远程输入（RX）的刷新软元件设置为X1000；将远程输出（RY）的刷新软元件设置为Y1000；将远程寄存器（RWr）的刷新软元件设置为D1000；将远程寄存器（RWw）的刷新软元件设置为D2000；将特殊继电器（SB）的刷新软元件设置为SB0；将特殊寄存器（SW）的刷新软元件设置为SW0。

（3）主站PLC

CPU的软元件和本地站PLC CPU的软元件之间的关系。经上述设置其输入输出I/O关系如图4-20所示。图中阴影部分指的是实际应用的软元件。寄存器、特殊继电器及寄存器之间也有对应关系，具体略。



图 4-24　用于运行程序

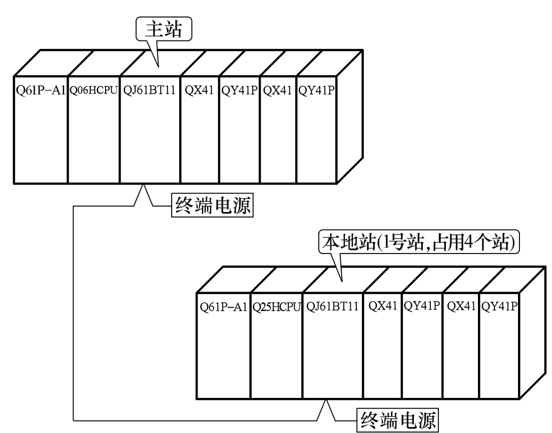


图 4-25　主站与本地站相连系统配置

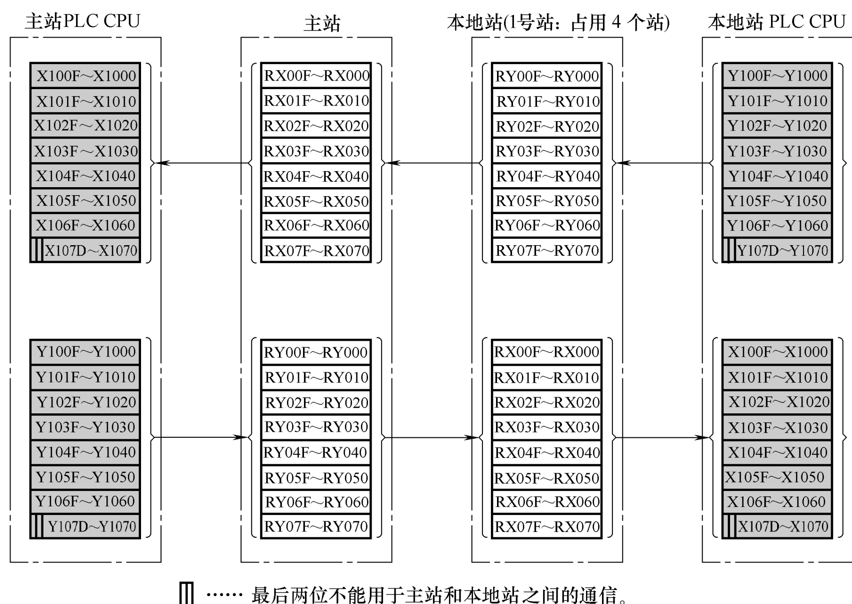


图 4-26　主站 PLC CPU 的软元件和本地站 PLC CPU I/O 之间的关系

（4）创建一个程序

有了图 4-26 关系，就可按启动循环通信、实现数据链接及执行读取缓冲存储器及实现用户对控制的要求编写程序。图 4-27 所示为主站控制程序。图 4-28 所示为本地站控制程序。

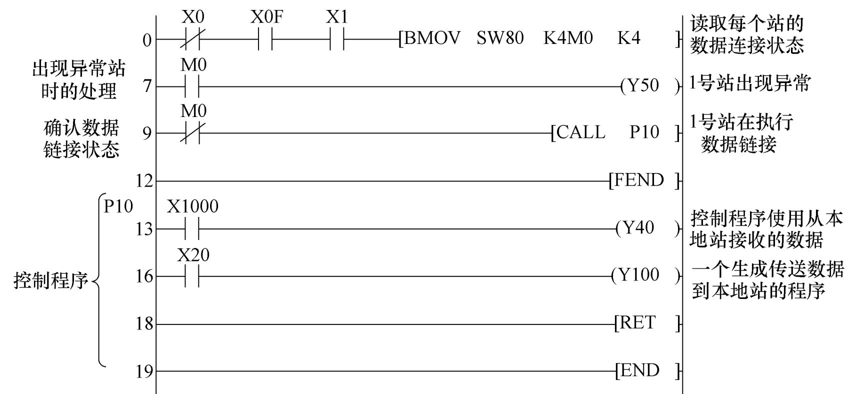


图 4-27　主站控制程序

（5）执行程序

首先接通远程 I/O 站的电源，然后接通主站的电源，启动数据链接。之后可用主站及本地站的 LED 显示器确认运行情况。图说明了当正常执行数据链接时，主站和远程 I/O 站的 LED 显示状态。也可利用控制结果看是否能达到要求确认网络工作正常。

4. 主站与现场设备站相连

（1）系统配置

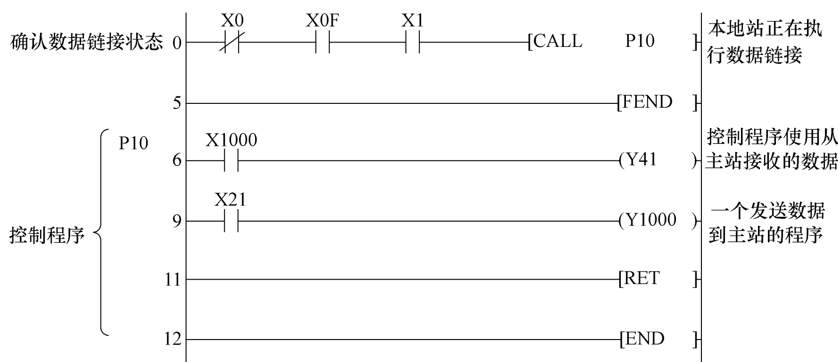


图 4-28　本地站控制程序

图 4-29 所示为本例系统配置及站号指定。这里的现场设备站为 AJ65BT-R2 RS-232C 接口模块，用以连接条形码阅读器，读取数据，并通过连网传给 PLC。

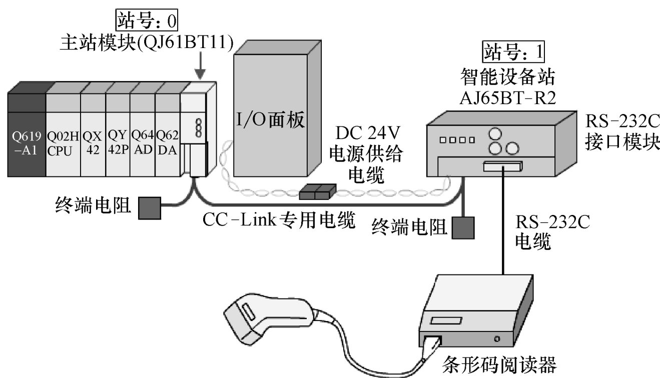


图 4-29　主站与现场设备站系统配置例

（2）系统设置

主站硬件设置站号为 0（主站），传输速率为 156kbit/s，方法同本小节介绍的主站与远程站配置实例。现场设备展硬件设置如图 4-30a 所示，站号为 1，传输速率为 156kbit/s。现场设备站与条形码阅读器串口的波特率、数据位、校验位也要设置。两者设置要一致。图 4-30b所示为现场设备站 AJ65BT-R2 设置示意。

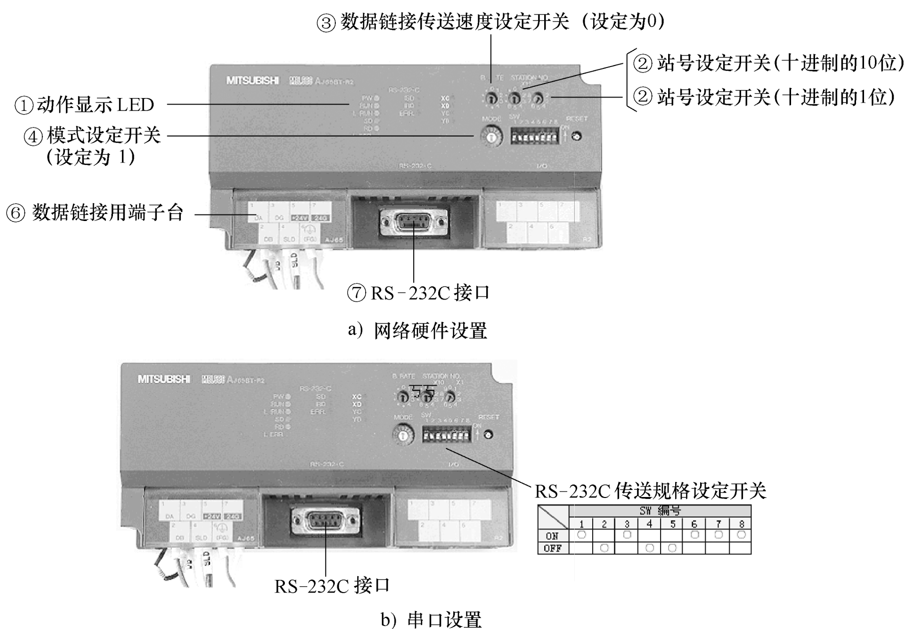
本例使用的条形码阅读器为东研 TCD-400/TBR-400。其开关状态设置如图 4-31 所示。

根据这个设置条形码阅读数据格式如图 4-32b 所示，而图 4-32a 所示为可用的两种条形码。

主站及从站网络参数设置也是用编程软件。主站设置为：站号为 0，连接模块数为 1，模式设置为在线（远程网络模式），所连接的从站信息指定为现场设备站。从站设置为：站类别为“现场设备站”，站号为 1，占用站数为“1 站”，智能站用缓存的指定为“自动：1536 字”。

（3）创建程序

由于与本现场设备设置循环传送得到的远程输入、输出（RX、RY）只是控制信号，没有输入输出数据。所以要读取条形码数据，要运用循时传送。这就要创建与执行相应的顺序程序。图 4-33 所示为创建这程序的流程。



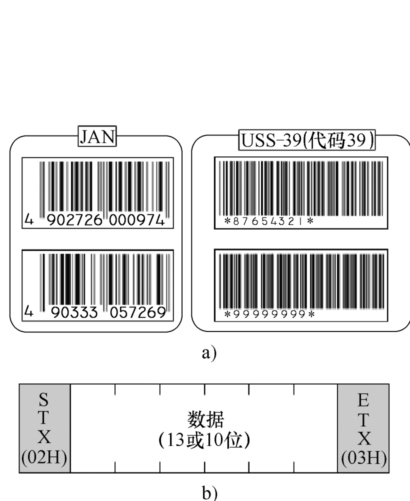
	SW 编号							
	1	2	3	4	5	6	7	8
ON	○		○			○	○	○
OFF		○		○	○			

图 4-30　现场设备站 AJ65BT-R2 设置示意

设定开关		设定开关的状态·内容		
1	OFF	传送速度(9600bit/s)		
2	OFF			
3	ON			
4	OFF	校验(偶数)		
5	OFF	终端电阻STX/ETX		
6	ON	条形码类型JAN	ON	条形码类型USS-39(代码39)
7	ON		OFF	
8	ON		OFF	
9	OFF		OFF	
10	OFF		OFF	

数据位长(7位)和停止位长(2位)固定不变，因此无设定开关。

图 4-31　条形码阅读器状态设置示意



注)10位时的最初和最后为“*”。

图 4-32　条形码及其阅读数据格式

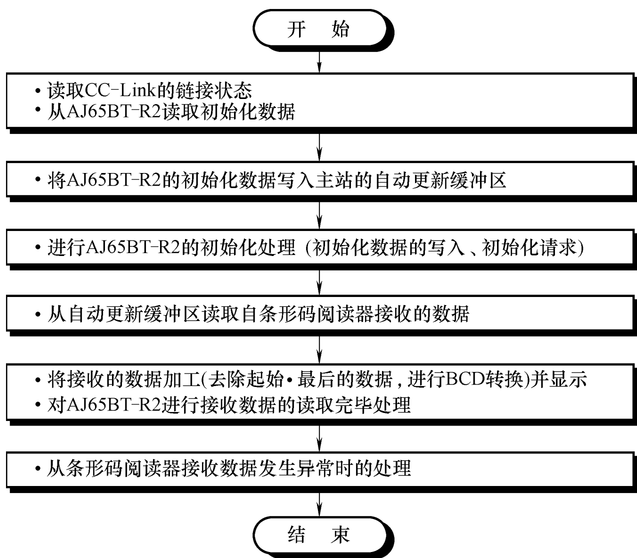


图 4-33　创建程序流程

本例引自三菱公司在线培训系统（e-learning）“CC-Link 基础”课程课题 7。具体程序及程序执行效果说明请参看该培训系统。这里略。

4.3 DeviceNet

关键词：显性位、隐性位、仲裁、仲裁标识、载波侦听逐位仲裁、显式连接、隐式连接、生产者/消费者模式、查询（Polled）、循环（Cyclic）、状态改变（Change of State，COS）

DeviceNet 是数字、多分支的网络，用以连接控制器、I/O 部件相互通信。是多点传送（一对多）的点对点、多主站和主/从网络。每个控制器或 I/O 部件即为网络上的一个站点。也是生产者（提供通信数据站点）、消费者（消费通信数据站点）的网络，支持多通信层次与信息优化。本质上讲，它还是运行在低成本的 CAN 总线上的 CIP 网络。

4.3.1 DeviceNet 简介

1. DeviceNet 组成

其组成如图 4-34 所示。

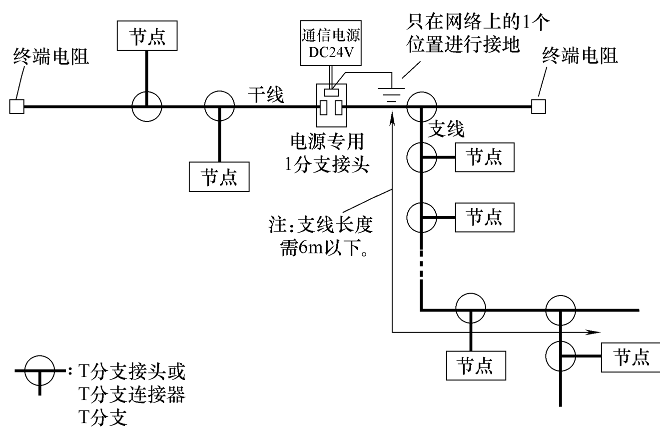


图 4-34　DeviceNet 组成

从图知，它由站点、干线（还有支线）、通信电源及终端电阻组成。

1）站点。包括连接外部 I/O 或智能控制器的从站及管理 DeviceNet 并协调各从站通信的主站。一个网络必须有一个主站，但也可有多个主站。网络站点最多可达 64 个。主站位置无需位于网络的一端，可处网络的任一位置。由于主站的位置不固定，因此更便于配线。

2）干线、支线。所谓干线，是指在两端安装了终端电阻的一段电缆。而从干线分支出来的电缆均为支线。DeviceNet 的干线、支线均使用专用电缆。电缆内含两对双绞线，其中一对为信号线，一对为电源线，此外还有屏蔽线。

3）电源为 24V 标准直流电源。用以向网络各个站点供电。电源可在网络的任何地方接入，还可配备冗余电源。

4）DeviceNet 要求在干线的末端安装终端电阻，而不可安装在支线末端。电阻的要求为 121Ω、1% 金属膜及 1/4W。

2. DeviceNet 网络模型结构

与 CompoNet 一样，对照 OSI 模型，它也仅有 4 层，即物理层，数据链路层，传输网络层及应用层。它的物理层与数据链路层沿用了 CAN 协议标准。

（1）物理层

包括两部分，介质访问单元和传输介质。介质访问单元由驱动器、收发器、误接线保护回路、调压器和可选的光隔离器和其他用于连接站点到传输介质的电路组成。在 OSI 模型中被称之为物理介质访问。物理层还包括连接传输介质的电气及机械接口的定义。

DeviceNet 物理层和介质有下列特征：使用 CAN 技术；尺寸小、成本低；线性总线拓扑结构；支持 3 种传输波特率（125K 波特、250K 波特及 500K 波特）；使用含两对双绞线及屏蔽线、低损耗、低延迟的多种专用电缆（包括粗缆，多用作干线和细缆，多用于分支线）传送信号与 24V 直流电源；支持干线或支线的使用不同种类电缆；支线长度可达 6m；最多支持 64 个站点；站点接入、退出无须断开网络；误接线保护功能；可同时支持隔离和非隔离物理层；支持密封介质；在设备连接方式上，可以灵活选用开放、封装端头两种形式；支持有源和无源设备，对于有源设备，提供专门设计的带有光隔离的收发器，光电隔离可用于电压等级较高的设备（如驱动器、软启动器和电动阀门），等等。

DeviceNet 提供多种连接器，如图 4-35 所示。



a) 螺丝端口连接器　　b) 小型、微型可接插连接器　　c) 扁平电缆连接器

图 4-35　DeviceNet 连接器

DeviceNet 使用不归零（NRZ）编码。定义了两种互补的“显性”（Dominant，逻辑 0）和“隐性”（Recesive，逻辑 1）逻辑电平。同时传送“显性”和“隐性”位时，总线结果值为显性。

代表逻辑电平的物理状态的规定包含在 ISO 11898 标准中，如图 4-36 所示。对于一个脱离总线的站点，典型 CAN_L 和 CAN_H 的隐性（高阻抗）电平为 2.5V（电位差为 0V）；典型 CAN_L 和 CAN_H 的显性（低阻抗）电平分别为 1.5V 和 3.5V（电位差为 2V）。

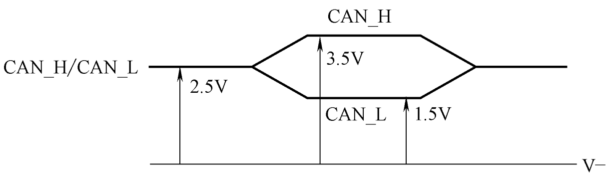


图 4-36　逻辑电平物理状态

它的位时间，即速率的倒数，由同步段、传播段、相位缓冲段 1、采样点、相位缓冲段等部分组成。如图 4-37 所示。

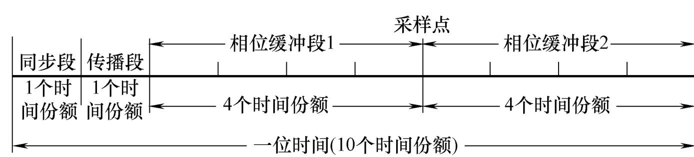


图 4-37　位时间组成

这里的同步段用于总线上各个站点，传播段用于补偿网络内的传播延时，相位缓冲段 1、相位缓冲段 2 用于补偿沿的相位误差。只有在采样点电平才被读出，并保留，以用于处理。

（2）数据链路层

DeviceNet 数据链路层用的也是 CAN 标准。尽管 CAN 定义有多种帧格式，如数据帧、远程帧、过载帧、出错帧等，但 DeviceNet 仅使用其数据帧，其格式如图 4-38 所示。

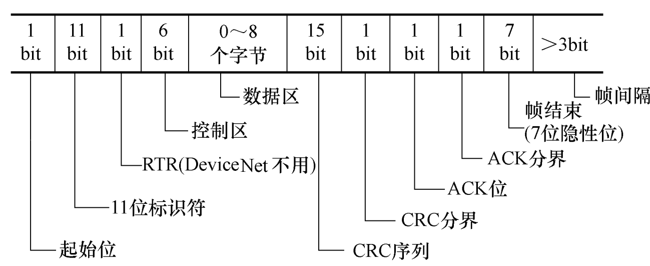


图 4-38　CAN 数据帧格式

从图知，它的帧结构有：

1）帧起始：标志数据帧的起始，它由单个“显性”位构成，在总线空闲时发送，在总线上产生同步作用。

2）仲裁标识：由 11 位标识符（ID10 ~ ID0）和远程发送请求位（RTR）组成，RTR 位为显位表示数据帧，隐位表示远程帧。标识符由高至低次序发送，且前 7 位（ID10 ~ ID4）不能全为隐性位，标识符用于提供关于传送报文和总线访问的优先权信息，其数值越小，表示优先权越高，发生冲突时优先发送。

3）控制区：由 6 位构成，前 2 位为保留位，为显性，后 4 位为数据长度码，表示数据场中数据的字节数，必须在 0 ~ 8 范围内变化。

4）数据区：由被发送数据组成，数目为控制场中决定的 0 ~ 8 个字节，第一个字节的最高位首先被发送。

5）CRC：包括 CRC（循环冗余码校验）序列（15 位）和 CRC 界定符（1 个隐位），用于帧校验。除了 CRC 校验，DeviceNet 还提供了位出错、应答出错、填充出错、格式出错检查。这些检查确保了它的通信稳定与可靠。

6）ACK：由应答位和应答界定符组成，共两位。

7）帧结束：由 7 位隐性位组成。

8）帧间隔：最少为 3 位。

CAN 是传输介质敏感的网络，即只有当其他站点不发送数据时，这个站点才能发送数据。为避免多点同时访问总线而又不产生冲突的办法是，采用非破坏性的、不损失带宽、不丢失数据的“位”仲裁。

其机理是，在总线空闲时，每个站点都可尝试发送；如果出现多于两个的站点发送，发送权的竞争通过 11 位标识符、采用载波侦听、逐位仲裁方法解决。网络上每个站点都拥有一个唯一的 11 位标识符。用其确定优先级的高低。11 位标识符数值最小的站点拥有最高的优先级。总线冲突仲裁时，优先级高的不受影响地继续传输数据，优先级低的则自动停止发送。所以这种碰撞和仲裁并未造成数据帧的损坏，不会浪费通信资源。由于标识符数值低的站点具有较高的优先权，所以对标识符的合理分配可使重要的数据得到优先发送。图 4-39 所示为两个站点总线冲突仲裁的一个实例。



图 4-39　两个站点总线冲突仲裁实例

该图所示有两个帧，其标识分别为 5E4H 和 5E8H（十六进制表示）。但仲裁到图示的“位”时，站点 1 为 0，而站点 2 为 1。按仲裁规则，站点 2 自动退出数据发送，而站点 1 则继续发送数据。而根据上述同时传送“显性”和“隐性”位时，总线结果值为显性的规则，在线上显示的仍为 0（显性），所以，不影响站点 1 的发送。

（3）网络传输层

与 CompoNet 一样，DeviceNet 也有网络传输层。其功能也是用以处理网络桥接与路由及报文分割与重组。

DeviceNet 的一个站点与另一个站点通信之前必须先建立关系（Relationship，也称连接、Connection）。这连接可通过 UCMM（Unconnected Message Manager）或未连接口组 2（Group 2 Unconnected Port）建立。此外，DeviceNet 支持显式（Explicit）与隐式（Implicit，常称为远程 I/O 通信）两种通信。显式通信基是基于“请求”与“响应”的通信，与系统配置及数据采集相关，实时性要求不那么严格。而隐式通信则是实时性要求很高的远程 I/O 通信。

站点可能是服务端，或客户端，或两者兼有。而服务端、客户端，都可以是数据的生产者，或消费者，或两者兼有。典型的客户端连接是产生“请求”，并消费“响应”。典型的服务端连接是消费“请求”，并产生“响应”。依此，DeviceNet 有多种模式。例如，一些客户端或服务端连接可能仅仅是消费循环或状态改变的信息。相反，另一些客户端或服务端连接可能仅仅是生产这些循环或状态改变的信息。使用好这循环或状态改变有关的连接可大大减少对网络带宽的要求。

不管什么时候与其他站点通信，首先要通过 UCMM 或未连接接口组 2 建立显式信息连接。这个显式连接可用以从一个站点向另一个站点传送数据，或用以建立隐式连接，即远程 I/O 通信连接。一旦一个远程 I/O 通信连接建立，11 位 CAN 标识区将作为这个数据的唯一标识。这时这个帧的其余部分包含的将不再是协议数据，而只是应用数据。当应用要求传送信息多于 8 位数据时，它可利用 DeviceNet 帧分割协议，以将信息分称几个相继的帧传送。

为了充分发挥 DeviceNet 的生产者、消费者这样机制的好处，它的唯一的连接 ID 是严格控制的。为此，见表 4-7 所示，DeviceNet 用 11 位 CAN 标识去定义连接 ID，并划分这 11 位为 4 组。头 3 个定义组含 2 个区。一个 6 位的区用作媒体访问标识（MAC ID），而其他则作为信息 ID。这两个区的组合就是这连接的 ID。在 DeviceNet 上的站点要负责管理自身的标识。这站点自身标识是按信息优级分配，而无视它的 MAC ID。凭借复制 MAC ID 算法，即使没有中心管理工具与记录，CAN 标识的唯一性也可得到保证。表 4-7 所示为 DeviceNet 分布的 11 位 CAN 标识区。

表 4-7　DeviceNet 分布的 11 位 CAN 标识区

标识位											十六进制范围	使　用
10	9	8	7	6	5	4	3	2	1	0		
0	Group 1 Message ID				Source MAC ID						000 ~ 3FF	Message Group 1
1	0	MAC ID						Group 2 Message ID			400 ~ 5FF	Message Group 2
1	1	Group 3 Message ID			Source MAC ID						600 ~ 7BF	Message Group 3
1	1	1	1	1	Group 4Message ID (0 ~ 2f)						7C0 ~ 7EF	Message Group 4
1	1	1	1	1	1	1	×	×	×	×	7F0 ~ 7FF	非法 CAN 标识
10	9	8	7	6	5	4	3	2	1	0		

由于 DeviceNet 的标识含有站点 MAC 地址，所以可自动避免标识重复。此外，DeviceNet 站点管理自身标识关键的好处是：站点可在任意时间加入或退出网络；可在任意时间增加现有站点间的点对点通信，或两者兼有，而无须弄清现有的设置。由于各站点都知道那些 ID 已经在使用，所以，在两个站点之间加入一个 I/O 连接，如指明优先级、数据路径及数据生成的激励等，所要求的做的也就很简单了。

（4）应用层

也即 Devicenet 的高层，使用的也是 CIP 协议。CIP 使用生产者/消费者模式传输数据。信息是以连接的 ID 作为标识，允许多站点共同消费基于唯一连接 ID 的站点所生产的相关数据。而不像传统的源/目标模式那样，靠指明源与目标地址，在源与目标之间一一传送。具体讲，这种模式的好处是：

假如一个站点要接收数据，只要提出消费数据的要求；

假如第 2 或 3、4、等个站点也要接收这个数据，这些站点要弄清的只是要可同时接收这个数据的连接 ID。

总之，在这种模式下，生产者作为数据源在总线上广播数据，任何站点都可以同时消费这个数据，多站点使用数据也只需广播一次，因此节省了网络带宽，提高了网络的效率。

CIP 的严格面向对象及它的网络间无缝桥接与路由问题，在 CompoNet 中已有介绍，这里不再赘述。

此协议落实到 DeviceNet 还有就是，使用称之为预定义主从连接集合（Predefined Master/Slave Connection Set）。具体讲就是，一个基于主从关系、可变、简化的通信机制。其中也含有最常用的 I/O 数据的打包与传送。

DeviceNet 的一个关键优点是，它是“电源接通”网络。符合它的规范的传感器、操作器都设计成具有“接通电源”预定义功能。这样，当“电源接通”时，这些部件将知道将

要生产与消费的数据类型及数量。同时，上述预定义的主从连接集合则提供几乎配置完整的连接对象。这样，“电源接通”后，仅有的步骤只是主站向预定义集内属于它的从站提出传送数据请求，从站则生产有关类型的数据。具体数据类型取决于从站配置与应用的要求。

这有关类型数据有：查询（Polled）、循环（Cyclic）、状态改变（Change of State，COS）。

查询：在循环方式下，从站接收来自主站按顺序定义在主站扫描表中的输出数据；同时传送它的输入数据，以响应主站的查询请求。主站的查询速率取决于：在扫描列表中的站点数、DeviceNet 波特率、主站及其列表中从站生产的信息量及主站定时间隔。对给定的系统配置，这通信方法具有确定性。这里输出数据是单播的，而输入数据可能是多播的。

循环：在循环方式下，站点准确地按预定义的时间间隔生产数据。允许每个使用者按其应用要求选择合适的时间间隔。这种模式可减少在总线上数据传输量，能更有效利用总线的带宽，适用于一些模拟设备站点。

状态改变：在状态改变方式下，站点根据它的状态改变或基于心跳率（Heartbeat Rate）生产数据。有了这个心跳率生产的数据，可使消费方知道生产方仍然在线并处激活状态。DeviceNet 还可调整参数，按用户习惯的设定心跳间隔，以优化带宽的利用。状态改变方式多用于离散的设备站点。

3. DeviceNet 拓扑结构

DeviceNet 可能的拓扑结构如图 4-40 所示。

从图知，它为总线结构。可建立各种分支。网络最多的站点数为 64 个。网络干线长度与波特率、线缆类型有关。DeviceNet 推荐使用的电缆有：粗缆、细缆、扁平电缆、电缆 Ⅰ 及电缆 Ⅱ。这些电缆电气、物理特性及适应环境不完全相同。但允许在干线系统中混合使用。有的使用特性也可换算。站点可以随机分配，还可不连续分配。但建议还是有地规则的分配为好，如主站为节点 63，从站为节点 1 ~62 而配置器为节点 0。表 4-8 所示为 DeviceNet 使用不同电缆时的波特率、线缆类型、拓扑距离间的对应关系。

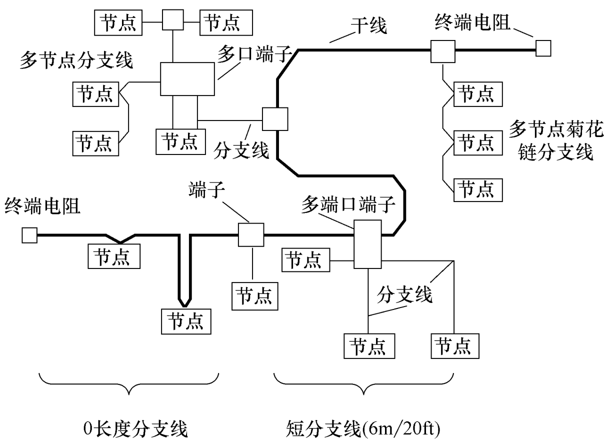


图 4-40　DeviceNet 拓扑结构

表 4-8　DeviceNet 波特率、线缆类型、拓扑距离间的对应关系

细缆：拓扑				
通信速率/(kbit/s)	干线长度/m(ft)	干线变换(粗缆)	累计支线/m(ft)	最长支线/m(ft)
125	100(328)	5.0	156(512)	6(20)
250	100(328)	2.5	78(256)	6(20)
500	100(328)	1.0	39(128)	6(20)
粗缆：拓扑				
通信速率/(kbit/s)	干线长度/m(ft)	干线变换(粗缆)	累计支线/m(ft)	最长支线/m(ft)
125	500(1640)	1.0	156(512)	6(20)
250	250(820)	1.0	78(256)	6(20)
500	100(328)	1.0	39(128)	6(20)

（续）

扁平电缆:拓扑				
通信速率(kbit/s)	干线长度/m(ft)	干线变换(粗缆)	累计支线/m(ft)	最长支线/m(ft)
125	420(1378)	n. a.	156(512)	6(20)
250	200(656)	n. a.	78(256)	6(20)
500	100(328)	n. a.	39(128)	6(20)
电缆Ⅰ:拓扑				
通信速率/(kbit/s)	干线长度/m(ft)	干线变换(粗缆)	累计支线/m(ft)	最长支线/m(ft)
125	100(328)	5.0	156(512)	6(20)
250	100(328)	2.5	78(256)	6(20)
500	100(328)	1.0	39(128)	6(20)
电缆Ⅱ:拓扑				
通信速率/(kbit/s)	干线长度/m(ft)	干线变换(粗缆)	累计支线/m(ft)	最长支线/m(ft)
125	500(1640)	1.0	156(512)	6(20)
250	250(820)	1.0	78(256)	6(20)
500	100(328)	1.0	39(128)	6(20)

4. DeviceNet 规格

DeviceNet 规格见表 4-9 所示。

表 4-9　DeviceNet 规格

项　目	规　格			
通信协议	符合 DeviceNet 标准			
编码	非归零(NRZ)			
总线拓扑结构 连接形式①	线性(干线/支线);电源和信号在同一网络电缆中 多分支方式、I 分支方式可组合使用(用于主干及支线)			
总线寻址	带多点传送(一对多)的点对点;多主站和主/从: 轮询或状态改变(基于例外)			
总线访问	CSMA/NBA 方式			
数据包/B	0~8 字			
通信速率/(kbit/s)	500/250/125			
通信媒体	专用电缆 5 芯(信号线 2 根、电源线 2 根、屏蔽线 1 根) 专用扁平电缆 4 芯(信号线 2 根、电源线 2 根)			
通信距离 专用电缆 5 芯使用时	通信速率/(kbit/s)	网络最大长度/m	支线长度/m	总的支线长度/m
	500	100 以下②	6 以下	39 以下
	250	250 以下②	6 以下	78 以下
	125	500 以下②	6 以下	156 以下
通信距离 专用扁平电缆 4 芯使用时	通信速率/(kbit/s)	网络最大长度/m	支线长度/m	总的支线长度/m
	500	75 以下	6 以下	35 以下
	250	150 以下	6 以下	48 以下
	125	265 以下	6 以下	135 以下
通信电源	从外部提供 DC24V 的电源			
最多连接节点数	64 台(含主站、从站、配置器)			
系统特性	支持设备的热插拔,无需网络断电			

①干线的两端需安装终端电阻。

②干线使用较粗的专用电缆时的值。使用较细的专用电缆时为 100m 以下。

5. DeviceNet 特点

（1） 接线方便

使用专用电缆可进行 T 分支及支线分支等自由配线。有助于缩减现场的配线成本及维

护成本。

（2）网络开放

通信协议、规格开放化。对设备行规有详细定义，并用 EDS（遵循开放规范设备硬件描述）文件描述，使用时可将其集成（加载）进相应网络管理软件中。因此能够连接国内外不同厂家的 DeviceNet 兼容设备。而且只要选用合乎行规的厂商产品，即可保证多环境下设备的兼容性和互换性。

（3）模式多样

可主/从、多主/从、点到点或者三者的组合来组建网络。多主/从配置时其主站个数不受限制。主站被用来控制次要的设备。在一个通信链路上，只有主站能建立对通信进行初始化。从站只能收集从主站发出来的命令。一个主站还能作为另一个主站的从属站，而作为从属站后它仍可以有自身的从站。

（4）通信多样

DeviceNet 不仅能够进行远程 I/O 通信，数据互锁（点对点链接），还能够进行报文通信。可通过报文通信进行设备的设定及监控。再就是它的通信可使多个站点同时从一个数据生产者获得数据，既容易使站点之间数据获得同步、达到更精确的系统控制性能，又能够减少数据交换的次数，充分利用网络的带宽。

4.3.2　AB DeviceNet 组件及配置实例

1. AB 公司的 DeviceNet 组件

AB 公司是 DeviceNet 技术的开发者与主要生产者、其有关产品最为齐全。品种、类型、规格都很多。很容易按组网需要具体选用。其主要产品有 4 类：

1）控制器及其 DeviceNet 接口。类型很多，表 4-10 所示为 Logix5000 系列控制器及其 DeviceNet 接口。

表 4-10　Logix5000 系列控制器及其 DeviceNet 接口

特　　点	MicroLogix 1500	CompactLogix	FlexLogix	ControlLogix
内存(最大) 1 字 = 10Logix 字节	14K	1.5M 字节	512K 字节	8M 字节
I/O(最大)	最多 256 点 包括嵌入式和本地扩展	本地扩展最多 30 个 Compact I/O 模块，最大点数取决于控制器的内存	512 点(数字量)或 128 点(模拟量)，或者是二者的混合	最多 128000 点(数字量)或最多 3800 点(模拟量)，或者是二者的混合
本地 I/O	嵌入的和 1769Compact I/O	1769Compact I/O	1794 FLEX I/O 1797 FLEX ExI/O	1756 I/O
适用接口	1761-NET-DNI (MicroLogix1000、1200 和 1500)，I/O 控制 1769-SDN (MicroLogix 1500 only)	1769-SDN	1788-DNBO	1756-DNB

2）计算机 DeviceNet 接口卡。可通过 RSLinx 及 RSNetWorx for DeviceNet 软件接入 DeviceNet，监视数据、组态网络和设备。其主要产品及技术指标见表 4-11 所示。

表 4-11 计算机 DeviceNet 接口

如果用户计算机	选 择	目 录 号	技 术 指 标
有 PCMCIA 插槽,并且想要将计算机作为 DeviceNet 网络上的一个节点,用于编程监视,并组态网络,或者用于维护及故障诊断	DeviceNet PCMCIA 通信接口卡 网络入口电缆 开放式 5-针探头电缆,2. 5m 密封型、T 形电缆,2m(6ft) 密封的小型-插入式电缆,2m 5-针直线型插头	1784-PCD 1784-PCD1(定购卡时已经包括,但也可以单独订购) 从下列目录号中选择: 1787-PCABL 1787-MCABL 1787-TCABL 1787-PLUG1	• 在 Windows 95/98ME/NT/2000/XP 环境下驱动
具有 5V PCI 插槽,并且想要将计算机作为 DeviceNet 网络上的一个节点,用于编程、监视,并组态网络,或者用于维护及故障诊断	DeviceNet PCI 通信接口卡	1784-PCID	• 在 Windows NT/2000 环境下驱动
具有 5V PCI 插槽,并且想要将计算机作为 DeviceNet 网络上的一个节点,用于控制 I/O,编程、组态网络或者通过 SoftLogix5800 控制器控制 I/O	DeviceNet PCI 总线扫描器卡	1784-PCIDS	• 在 Windows NT/2000/XP 环境下驱动 • 主/扫描器 • 支持轮询、状态改变,周期和位选通通信 • 使用 IOLinx Software Development Kit(SDK IOLinx 软件开发工具)作为软件(如 SoftLogix ,客户 VisualBasic 程序,以及客户 VisualC + + 程序)的 I/O 应用接口
使用小尺寸,CompactPCI 总线,并且想要将计算机作为 DeviceNet 网络上的一个节点,用于控制 I/O,编程组态网络或者通过 SoftLogix5800 控制器控制 I/O	DeviceNet Compact PCI 总线扫描器卡	1784-CPCIDS	• 在 Windows NT/2000/XP 环境下驱动 • 主/扫描器 • 支持轮询、状态改变,周期和位选通通信 • 使用 IOLinx Software Development Kit(SDK IOLinx 软件开发工具)作为软件(如 SoftLogix ,客户 VisualBasic 程序,以及客户 VisualC + + 程序)的 I/O 应用接口
台式机或笔记本电脑,并且想要将计算机作为 DeviceNet 网络上的一个节点,用于控制 I/O,编程和组态网络	DeviceNet RS-232 个人计算机接口 DeviceNet RS-232 个人计算机接口,带全球 9V 直流电源适配器 U. S. 9V 直流电源适配器 开放式,5-针探头电缆,2. 5m 密封型,T 型电缆,2m 密封的小型-插入式电缆,2m 5-针直线型插头	1770-KFD 1770-KFDG 1787-USADPTR 1787-PCABL 1787-TCABL 1787-MCABL 1787-PLUG10R	• 在 Windows 95/98ME/NT/2000/XP 环境下驱动

3）I/O模块及其他器件。有分布I/O及基于机架I/O。其他器件有传感器等。表4-12所示为常用的一些模块。表4-13所示为一些可在特殊环境下使用的传感器。

表4-12　常用I/O模块

选择I/O	选择适配器	技术指标
分布式模块式I/O		
1734 POINT I/O	1734D POINTBlock I/O 1734-ADN 1734-ANDX(支持子网连通性) 1734-PDN(DeviceNet电源)	• 高度模块化(可混合,与用户的精确需求匹配) • 可拆卸端子块 • 具有带电插拔(RIUP)的特点 • 易于分散 • 全范围的数字量、模拟量、专用,以及温度模块 • 可达252点/每个适配器
1794FLEX I/O	1794-ADN	• 电子模块和端子块基座可分离设计 • 具有带电插拔(RIUP)的特点 • 24/48V直流 • 120/230V交流 • 继电器输出、模拟量、温度、专用、计数器及系列模块 • 2~32点/模块密度
1797 FLEX Ex I/O	1794-ADN (在防爆场合配用1797-BIC和1797-CEC)	• 用在防爆场合的具有本征安全的I/O • 独立于端子块基座的模块 • 具有带电插拔(RIUP)的特点 • 数字式(NAMUR)模拟量、温度、频率 • 2~16点/模块
1798 FLEX Armor I/O	1798-ADN 还要有以下产品配合: • 1798-DFTP1 (用于12mm DeviceNet电缆插头的终结器) • 1798-DFTP2 (用于18mm DeviceNet电缆插头的终结器)	• 在机器上安装 • IP67和NEMA 4X标称值 • 户外应用 • 24V直流模拟量和数字量 • 4点和8点/模块;可达64/节点
基于机架的I/O		
1769 Compact I/O	1769-ADN	• 类似于机架的I/O • DIN-导轨或面板安装 • 24V直流 • 120/230V交流 • 模拟量、温度、专用、计数器及系列模块

表4-13　可在特殊环境下使用的传感器

要在下面环境内使用传感器	选　择	技术指标
恶劣环境,如酒厂和食品加工厂,温度达70℃,或者高压冲洗和许多难闻溶剂场合	SmartSight 9000 传感器	• NEMA 6P,IP67,1200psi冲洗等级 • 选择微型或小型连接器,或者一条附加2m CPE支线电缆 • I/O逢变则报和位选通通信
要求较短检测距离的材料处理和包装工业	RightSight 光电传感器	• NEMA 4X,IP67,1200psi冲洗等级 • I/O逢变则报和位选通通信
潜在腐蚀环境,如金属加工、食品加工和材料处理工业	Bulletin 871™ 感应式接近传感器	• 1200psi(8,270kPa)冲洗等级 • 可使用小型或微型QD,或者2m CPE外套管电缆 • I/O逢变则报和位选通通信

（续）

要在下面环境内使用传感器	选　　择	技术指标
要求重载指示等级、多功能和耐恶劣环境、不透油结构的应用场合。该传感器的专利 3-路轴密封设计提供优良的抗液性	Bulletin 802DN 限位开关	• NEMA 13 和 IP65(IEC529)防护等级 • 可使用小型或微型 QD,或者 2m CPE 外套管电缆 • I/O 逢变则报和位选通通信,并且内置 Devicenet 连通性
要求直接连接到 DeviceNet 以得到高级功能,同时降低接线费用的应用场合	Bulletin 842D 绝对值型多功能旋转编码器	• NEMA4,13 和 IP66(IEC 529)防护等级 • 五-针微型快速切断 • 可使用小型或微型 QD,或者 2m CPE 外套管电缆 • I/O 逢变则报和位选通通信

此外还有操作员接口，电机起动器/保护器，变频器，运动控制器、桥接设备等。总之，它的从站组件很多，可用于不同的场合，以满足不同的要求。而且发展变化也很快。所以实际选用时，可向有关厂商具体咨询。

4）通信介质及网络附件。这些组件品种、类型、规格最多，配置时还不能丢项，可按需细致选用。

5）软件。要用到的主要软件有编程软件及网络监控机配置软件。对 Logix500 系列机（含 ControlLogix 机）具体是：RSLogix5000、RSLinx 及 RSNetWork for DeviceNet。RSNetWork for DeviceNet 可用以作脱机配置，也可联机读取网络。

2. AB DeviceNet 网络配置实例 1

本例有 8 个站点。其中主站有 3 个（其中一个设置为从属主站）。从站 5 个。其脱机配置大体有如下步骤：

（1）运行 RSNetWork for DeviceNet 软件

在其主菜单“File”下的“New”项。之后将使 DeviceNet-RSNetWork for DeviceNet 出现空白（没有站点）的一个网络。

（2）添加站点

在空白网络上添加所有主、从站点。办法是，从左方的“Hardware（硬件）”窗口上，选择所需的硬件拖放到主窗口的空白网络上。

如图 4-41 所示，这里已拖放了 8 个站点。01、02、03 为控制器模块，可作为主站点或从属主站点。后者可用于控制器间连锁配置。其他 5 个位从站模块，只能作为从站点。

上述添加后的网络是用图形表示的，也可用目录（列表）表示。办法是，点击主窗口的主菜单项“View”下的“Mastr/Slave Configuration”项。将出现如图 4-42 所示目录表示的窗口。

在此窗口上，还可修改所作的配置。如删除或添加站点等。还可点击主窗口的主菜单项“View”下的“Graph”项，又回到用图形显示。

从图还可看出，这时网络站点哪个是主站，哪个是从属主站点，每个主站管理哪个从站，关系都不明确。为此，还须先确定那些站点可作为主站，哪个是从属主站点。然后再确定被主站管理的从站。

（3）确定哪些站点为主站模块

办法是用鼠标左键双击某个主站模块图标，或用右键点击某个主站模块图标，在弹出的下拉菜单上，点击“Properties（特性）”项。之后将弹出的与模块名相同的模块特性窗口。该窗

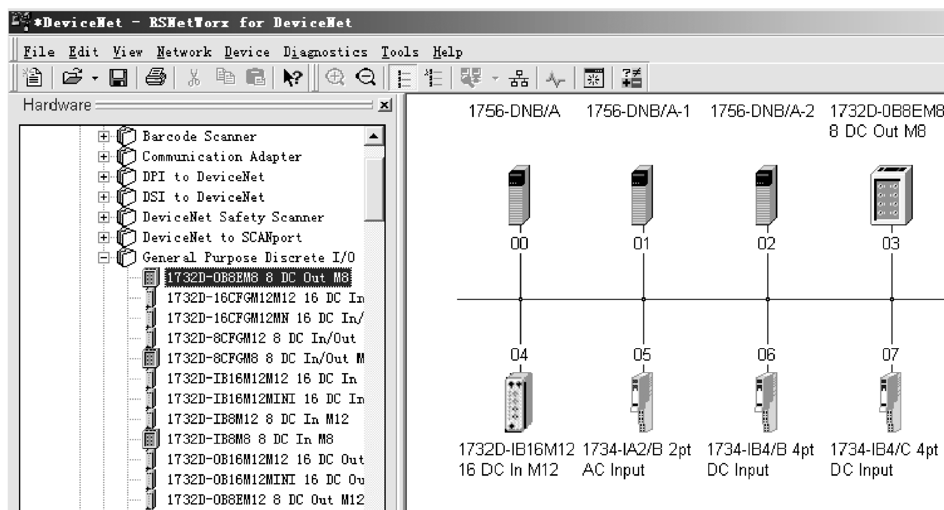


图4-41 已添加8个站点网络图形表示

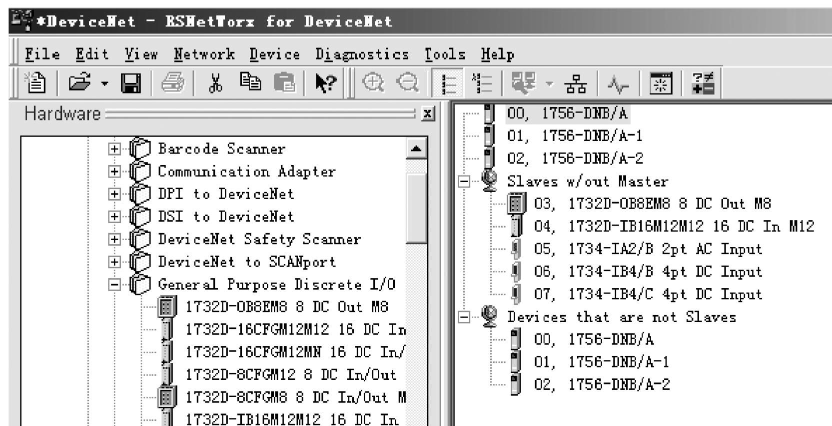


图4-42 网络站点目录表示

口有“General”、“Module”、“Scanlist”、“Input”、“Output”、“ADR”及“Summary”7个表单项。可点击选择对应的设置窗口。图4-43所示即为站点2的主站模块模式设置窗口。

该窗口用于主站模式设置。为此，可点击按钮“Slave Module”。之后将弹出如图4-44所示从属主站设置窗口。如果点击在其上“Enable Slave Mod”选择框（如图所示打钩），则该站点选定为从属主站，也用作为其他主站的从站（但它仍有主站功能，仍可为其配置从站）。进而再选择与从站功能有关的参数。其中各项含义见DeviceNet简介中的说明。选择完成后再点击“OK”按钮，则回到原主站模块特性模式设定窗口。

（4）选定主站建扫描表

确定受其管理的从站图4-45所示为点击“Scanlist（扫描表）”表单后出现的窗口。如在其左窗口(“Available Devices（可用部件)”）空白处点击鼠标右键，将弹出图示下拉菜单。如点击“Share（共享)”则图示处打钩，显示选定共享所有输入模块数据。本例有5个输入模块可供选择。也可不选共享，则已被别的主站选定后的从站或从属主站将不再作为可用部件，也不在此显示。

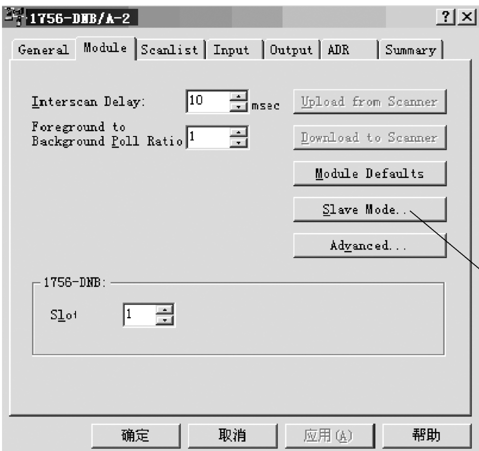


图 4-43　站点 2 主站模块特性模式设定窗口

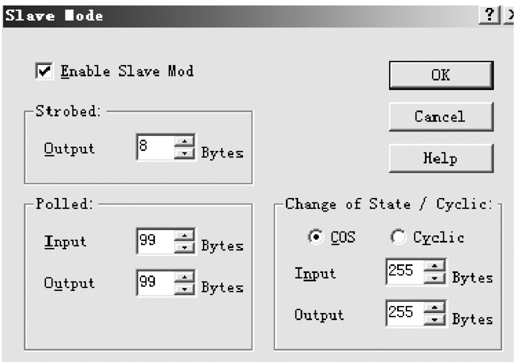


图 4-44　从属主站设置窗口

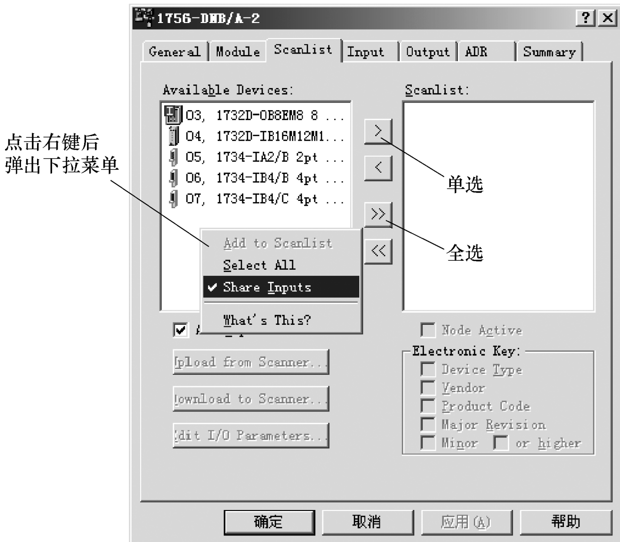


图 4-45　“Scanlist（扫描表）”窗口

图 4-46 所示为站点 0 的扫描表。这里以选定了站点 2 及一个输入模块。双击选定的“05，1734-IA/B 2pt”还将弹出如图所示编辑 I/O 参数窗口，可在其上编辑有关参数。

所有主站点扫描表都建完后，还可进入目录（列表）表示。如图 4-47 所示，这里指明不能作为从站的有两个，即站点 0、1（因为它们的模式不设为从站）。而且还可清晰地看出，各个主站各有各的从站。其中还有 2 个被共享输入的从站。

扫描表建成后，可进入输入输出设置。分别设置各个从站占用主站的地址，以便于编程使用。

（5）存储文件

完成所有设置后要存储文件。办法是点击主菜单项“File”下的“Save”或“Save as”项，在弹出的存储窗口上输入合适的文件名及选择合适的文件夹，再点击“保存”按钮，即可存储为扩展名为“dnt”的文件。在运行 RSLogix5000 编程软件。添加这里选定 Devi-

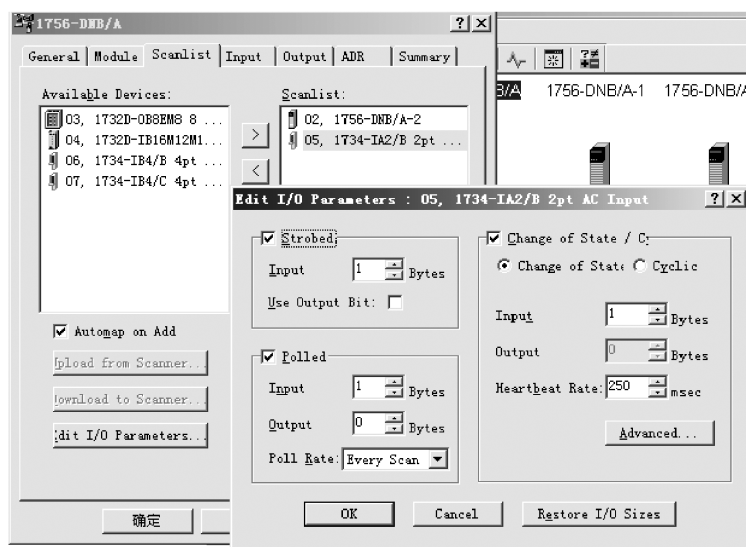


图 4-46　站点 0 的扫描表

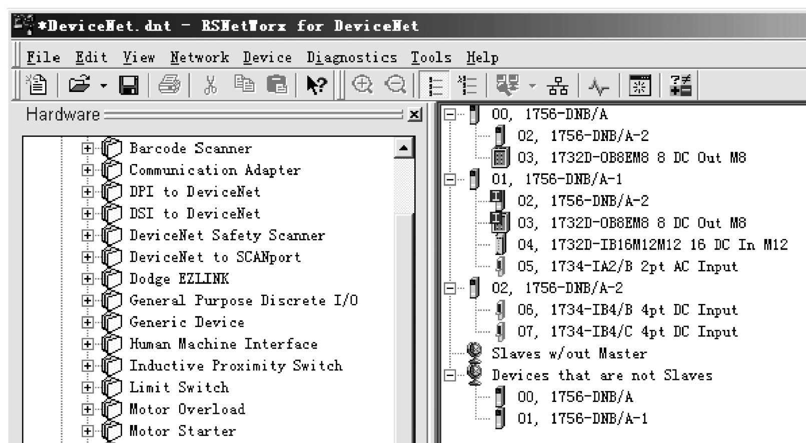


图 4-47　扫描表完成后网络目录（列表）表示

ceNet 模块后，可在模块特性的窗口的“RSNetwork”表单上，加载此文件，为编程使用。也可通过编程软件打开加载有此文件的“RSNetwork for DeviceNet”软件，回到本软件的网络窗口。

（6）联机下载

先确定访问网络的路径。办法点击主窗口的主菜单项“Network（网络）”下的“Properties（特性）”项。接着，在之后弹出窗口上，点击“Set Online Path”按钮，将弹出的“Brows for network”窗口。同时，缺省运行了 NetLinx 网络软件，由它寻找可能通信路径。这路径可通过串口或其他网络接口（如果计算机配置有这类接口）。当寻找完成将显示所有可能的路径。这时可选择合适的联网路径。之后可点击主菜单项“Network（网络）”下的“Online（在线）”项，如网络正确即可联机，进而下载设置。或上载现场网络及监视网络。

本例网络用的是手工配置，其实也可自动配置。后者可用“RSNetwork”下的“Devi-

ceNet Nod Commsioning Tool”站点调试工具及编程软件自动扫描网络，进而建立扫描表，完成网络配置。再，本例只是为了说明如何进行脱机配置而引用的。实际系统当然很少这么凑巧，真是这样的。

3. AB DeviceNet 配置实例 2

本例主站为 AB Controllogix PLC，使用 DeviceNet 1756-DNB 模块。从站有多个，都是采用图尔克设备。其 DeviceNet 通信接口（扫描卡）都是 BL67-GW-DN 模块。在与这接口对应机架上还有数字量输入模块 DI：BL67-8DI-P，输出模块 DO：BL67-8DO-0.5A-P 及模拟量输入模块 AI：BL67-2AI-I 及输出模块 AO：BL67-2AO-I 等。这几个站点地理上分布不同位置。本工程由沈阳鹭岛公司开发，用于国电康平发电有限公司废水处理系统中。图 4-48 所示为本系统的组成简图（只示出两个从站）。之所以这样配置主要是图尔克产品比较适合本例实际现场的需要。

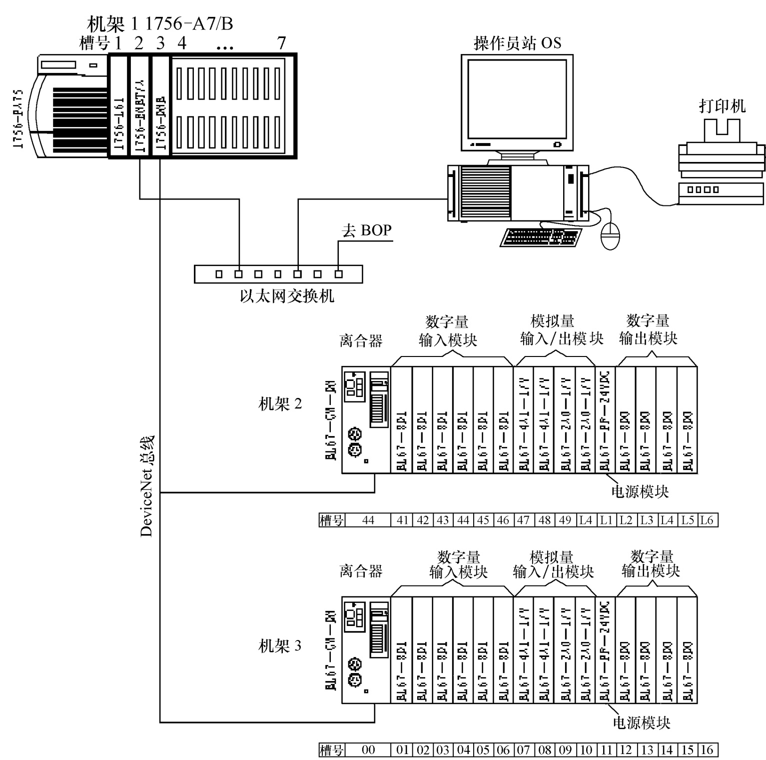


图 4-48　AB 主站图尔克从站 DeviceNet 系统组成

本例系统具体安装是：主站：AB PLC 电源模块安装在机架外面的左侧，其他模块安装在机架里面，可以插在任意槽位，所有 IO 模块完全支持带电热插拔。机架的槽位从 0 号开始，CPU 安装在 0 槽位，以太网通信模块安装在 1 槽位。DeviceNet 模块安装在 2 槽位。远程分站：DeviceNet 扫描器安装在最左侧，把拨码开关拨到设计图纸对应的站号，然后依次安装图尔克 IO 模块。

为方便计，本例先做好个站点的硬件设置，然后联机。用自动扫描方法，读取网络数据，以完成系统网络组态。其具体步骤是：

（1）软件组态及 IO 分配

打开RSLogix5000软件，在其上建立新工程，添加1756-A7（7槽）底板，添加1756-L62 CPU模块，添加1756-ENBT/A以太网模块，添加1756-DNB DeviceNet模块。有关DeviceNet模块的参数设置如图4-49所示。



图4-49　DeviceNet模块参数设置

从图知，这里主站的节点号默认为0。槽号为2。输入大小为远程DI、AI模块总点数，其中DI模块占一个字，AI模块每个通道占一个字。输出大小为远程DO、AO模块总点数，其中DO模块占一个字，AO模块每个通道占一个字。

除了DeviceNet模块设置，其他的当然也要设。所有设置完成后与PLC连网。本工程是通过以太网与PLC联网。为此，要在RSLinx里添加以太网通信驱动。其具体过程将在本书第5章介绍AB以太网时将有进一步说明。这里略。当然也可通过串口与PLC联网。与PLC联网后，把上述主站的设置下载给PLC。

（2）加载图尔克从站相关描述文件

由于图尔克从站不是AB产品。所以，还须把它的描述文件加载到RSNetWork for DeviceNet软件中。否则扫描结果看不到从站。为此要按如图4-50所示的目录，RSNetWork for DeviceNet软件打开“EDS Hardware Installation Tool”软件，进而在其上把“BL67-GW-DN”接口的描述文件加载到AB网络与编程软件中。

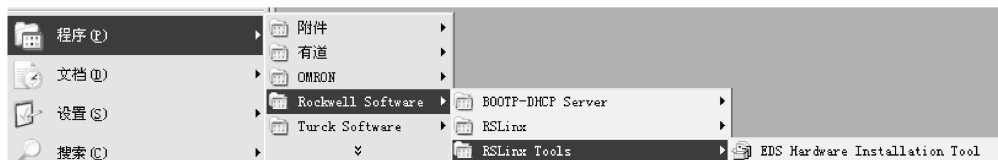


图4-50　RSNetWork for DeviceNet软件目录

（3）按要求对主站、从站硬件进行设置

做好模块安装与接线。接通电源。网络各站点处工作状态，全部在线运行。计算机也连网，并运行RSLinx软件。

（4）使用RSNetWork for DeviceNet软件在线扫描组态DeviceNet网络

具体方法是，运行RSNetWork for DeviceNet软件。然后如图4-51所示，点击“Network”菜单下的“Online”项，让网络在线。

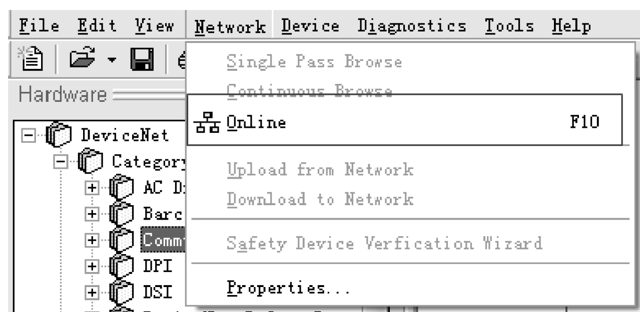


图 4-51 运行 RSNetWork for DeviceNet 软件让网络在线

之后系统将扫描网络。如果网络设置、安装、接线正确，将扫描到如图 4-52 所示的网络配置。

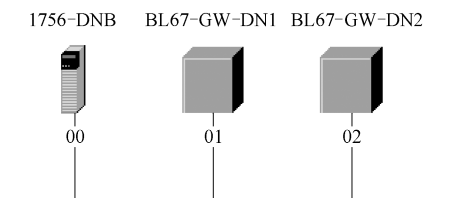


图 4-52 扫描到的网络配置
（实际这点多但这里只显示 3 个）

从图知，这里有三个站点，00 为主站。01、02 为从站（其他从站为示出）。首先双击 BL67-GW-DN1 进行配置。点击后将弹出如图 4-53 所示的“BL67-GW-DN”窗口。

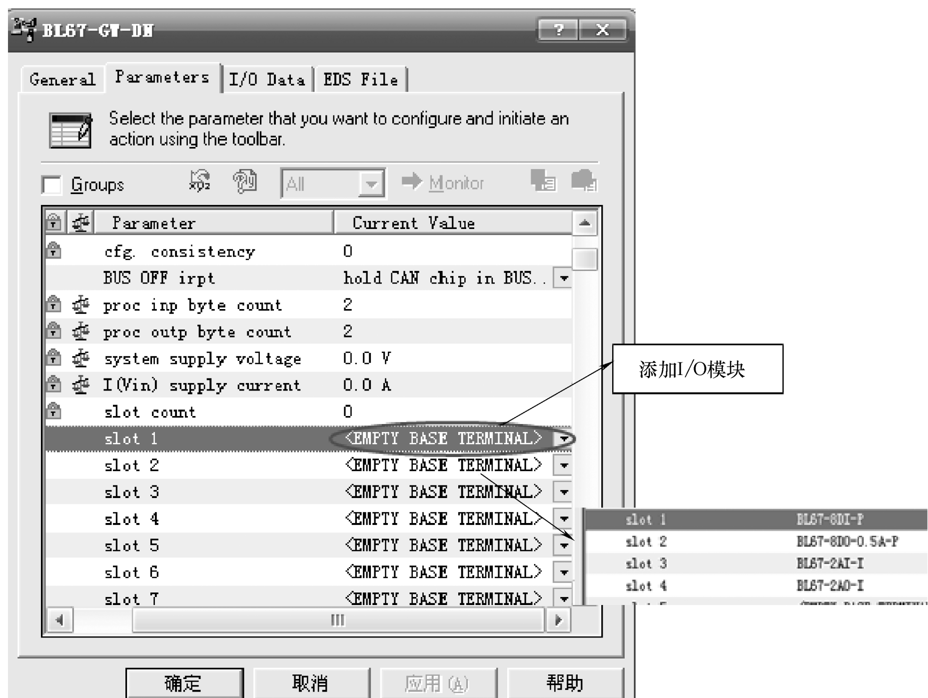


图 4-53 BL67-GW-DN1 窗口

在其上的 Parameters 表单上，按设计要求添加 I/O 模块。对 AI/AO 还需要对信号类型进行配置。如图 4-54 所示选用的输入为 4～20mA。

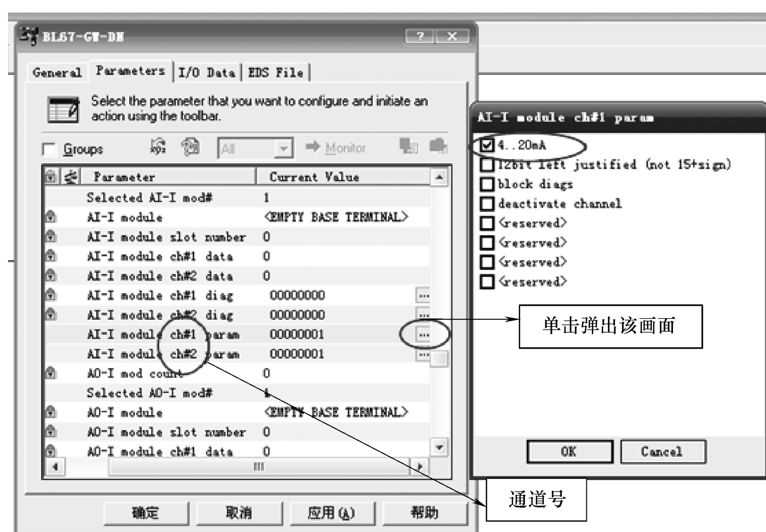


图 4-54　选用的输入为 4～20mA

接着进行远程分站起始地址分配。为此要双击 DNB 模块图标。进而将弹出如图 4-55 所示的“1756-DNB”对话框窗口，点击 Scanlist，显现 Scanlist 表单。再双击右侧方框内远程站扫描模块图标，弹出“Edit I/O Parameters：01，BL67-GW-DN”对话框窗口。从中选择 Chang of State/c 项。这里 Input 表示本站输入量的起始地址。Output：表示本站输出量的起始地址。

按照上述设计要求把各个远程站的 IO 设置完毕，下载到 PLC。保存配置。RSNetWork 至此配置完成

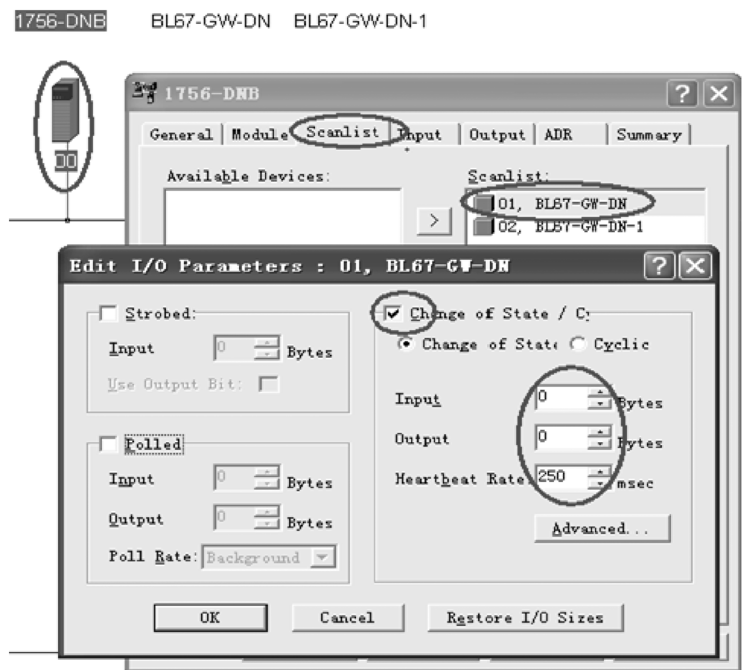


图 4-55　1756-DNB 等多个对话框窗口

（5）使用 RSLogix 5000 查找远程 IO 点地址

打开 RSLogix 5000 软件，点击全局标签，如图 4-56 所示。

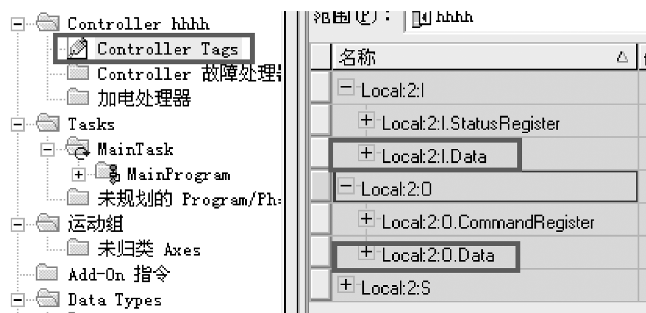


图 4-56　全局标签

从图知，远程分站所有输入量都在 Local：2：I. Data 里，输出量都在 Local：2：O. Data 里。起始地址在上述图 4-56Input 和 Output 中设定。有了地址 PLC 就按要求编程，可直接使用从站所有的数据了。

4.3.3　OMRON DeviceNet 组件及配置实例

1. 组件

（1）主站单元

表 4-14 列出 OMRON PLC 主要主站单元型号及使用特性。其功能有：

表 4-14　OMRON PLC 主要主站单元型号及使用特性

安装 PC 本体	单元型号	可安装位置	主站/从站功能	最多可安装台数	
				使用配置器时	无配置器时
CS 系列	CS1W-DRM21(-V1)	CPU 板/扩展板（CPU 高功能单元处理）	主站及从站	16 台	
CJ 系列	CJ1W-DRM21				
CVM1/CV 系列	CVM1-DRM21-V1	CPU 板/CPU 扩展板（CPU 高功能单元处理）	只有主站功能	16 台	1 台
CS 系列	C200HW-DRM21-V1	CPU 板/扩展板（高功能 I/O 单元处理）		16 台	
SYSMAC α 系列				10 台或 16 台	
C200HS				10 台	

1）远程 I/O 主站功能。与相应 CPU 单元配合可组成 DeviceNet 主站。有关使用性能见表 4-15 所示。

表 4-15　远程 I/O 主站功能使用性能

项　　目	装有主站的 CPU 单元	单元型号	无配置器时	使用配置器时
1 台主站连接从站的最多数量	CS 系列	CS1W-DRM21(-V1)	63 节点	
	CJ 系列	CJ1W-DRM21	63 节点	
	CVM1/CV 系列	CVM1-DRM21-V1	63 节点	
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1	50 节点	63 节点
	C200HS 系列		32 节点	63 节点

（续）

项　　目	装有主站的 CPU 单元	单元型号	无配置器时	使用配置器时
每台主站的最多控制点数	CS 系列	CS1W-DRM21(-V1)	2048 点 （IN 64CH/OUT 64CH） 或 16000 点 （IN 500CH/OUT 500CH）	32000 点 （5000CH ×4 块）
	CJ 系列	CJ1W-DRM21		
	CVM1/CV 系列	CVM1-DRM21-V1	2048 点 （IN 64CH/OUT 64CH）	6400 点 （100CH ×4 块）
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1	1600 点 （IN 50CH/OUT 50CH）	4800 点 （无报文） 1600 点 （有报文）
	C200HS 系列		1024 点 （IN 32CH/OUT 32CH）	1280 点
主站能够控制的每台从站的最多 I/O 点数	CS 系列	CS1W-DRM21(-V1)	IN 100CH ×2/OUT 100CH ×1	
	CJ 系列	CJ1W-DRM21		
	CVM1/CV 系列	CVM1-DRM21-V1	IN 32CH/OUT 32CH	
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1		
	C200HS 系列			
远程 I/O 分配区	CS 系列	CS1W-DRM21(-V1)	CS 用、CJ 用 DeviceNet 继电器区 或输入输出、数据存储器等的自由位置	输入输出、数据存储器等的自由位置
	CJ 系列	CJ1W-DRM21		
	CVM1/CV 系列	CVM1-DRM21-V1	DeviceNet 继电器区 （内部辅助继电器的特定区域）	输入输出、数据存储器等的自由位置
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1		
	C200HS 系列			

2）远程 I/O 从站功能。与相应 CPU 单元配合可组成 DeviceNet 从站。有关使用性能见表 4-16。

表 4-16　远程 I/O 从站功能使用性能

项　　目	装有从站的 CPU 单元	单元型号	无配置器时	使用配置器时
本从站的最多输入输出点数	CS 系列	CS1W-DRM21(-V1)	32 点 （IN 1CH/OUT 1CH） 或者 3200 点 （IN 100CH/OUT 100CH）	4800 点 （IN 100CH ×2/OUT 100CH ×1）
	CJ 系列	CJ1W-DRM21		
	CS 系列、SYSMAC α 系列	C200HW-DRT21	1024 点 （IN 32CH/OUT 32CH）	
	CQM1H、CQM1 系列	CQM1-DRT21	32 点 （IN 1CH/OUT 1CH）	
分配给装有本从站的 CPU 单元的区域	CS 系列	CS1W-DRM21(-V1)	CIO、WR、DM、EM、HR	
	CJ 系列	CJ1W-DRM21		
	CS 系列、SYSMAC α 系列	C200HW-DRT21	CIO、DM、EM、AR、LR、T/C	
	CQM1H、CQM1 系列	CQM1-DRT21	CIO	

3）报文通信功能。与相应 CPU 单元配合具有报文通信功能。有关使用性能见表 4-17。

表 4-17 报文通信功能使用性能

项 目	装有主站的 CPU 单元	单元型号	内 容
FINS 报文通信功能中每个主站单元可进行报文通信的最多节点数	CS 系列	CS1W-DRM21(-V1)	63 节点
	CJ 系列	CJ1W-DRM21	
	CVM1/CV 系列	CVM1-DRM21-V1	8 节点
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1	8 节点
	C200HS 系列		不能
Explicit 报文通信功能中每个主站单元可进行报文通信的最多节点数	CS 系列	CS1W-DRM21(-V1)	63 节点
	CJ 系列	CJ1W-DRM21	
	CVM1/CV 系列	CVM1-DRM21-V1	63 节点
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1	63 节点
	C200HS 系列		不能
报文最多长度	CS 系列	CS1W-DRM21(-V1)	SEND:267CH RECV:269CH CMND:542 字节 （依据指令代码）
	CJ 系列	CJ1W-DRM21	
	CVM1/CV 系列	CVM1-DRM21-V1	SEND:76CH RECV:78CH CMND:160 字节 （依据指令代码）
	CS 系列、SYSMAC α 系列	C200HW-DRM21-V1	IOWR:160 字节 （依据指令代码）

（2）从站单元

有：一般从站，输入、输出点数在 32 点以下；耐环境从站，使用圆形防水连接器接通通信电缆；模拟量从站，接入输入、输出模拟量；高功能从站，输入、输出大于 32 点，此外还具备其他功能；多 I/O 终端，多分支型拼接型从站。

还有智能从站，其类型很多。如带有 DeviceNet 接口的温控器、变频器。还有就是小型 PLC 从站，再如 CPM1A-DRT21 DeviceNet I/O 从站单元。它与相应 PLC CPU 配合可作为 DeviceNet 一个从站，允许主单元和 CPM2AH 之间有 32 点输入和 32 点输出数据交换。

（3）配置器

实际是计算机加专用插卡，再加 DeviceNet 配置器软件。运行后可作为 DeviceNet 的一个站点接入网络。可执行欧姆龙制造的主站单元的参数（扫描清单）设定及监控。此外，还可设定欧姆龙及其他公司生产的从站的参数。由于计算机可运行 CX-Integrator 网络管理软件，与 PLC 串口或其他手段连网后，也具有此功能，所以，它实际用处不大，不常用。

（4）电缆及连接器、分支器、终端电阻等网络附件

品种、类型及规格都很多，可按需要选用。

2. DeviceNet 配置实例

（1）1 个主站与 2 个远程 I/O 联网

配置 deviceNet 网络需要软件 CX-integrator。该软件在 CX-ONE4.0 集成包内。其配置过程如下：

1）运行 CX-integrator 软件，出现软件主窗口。后点击其上“插入”菜单项下的“网络”项，会出现如图 4-57 所示“向导-网络、组件”对话框。

在其上，选择“DeviceNet”项，选择后，点击“下一步”，将弹出如图 4-58 所示“向导-网络设置”窗口。



图 4-57　向导-网络、组件对话框



图 4-58　“向导-网络设置”窗口

在该窗口上点击“完成”，即完成了网络的建立。这时，在软件主窗口如图 4-59 所示，已建立了一个网络 1，为 DeviceNet 网络。但网络为空白的，其中没有一个组件。

2）插入组件（站点）。办法是，点击如图所示的“插入”菜单下的“组件”项。之后将组建会弹出如图 4-60 所示的“向导-网络/组建配置”窗口。

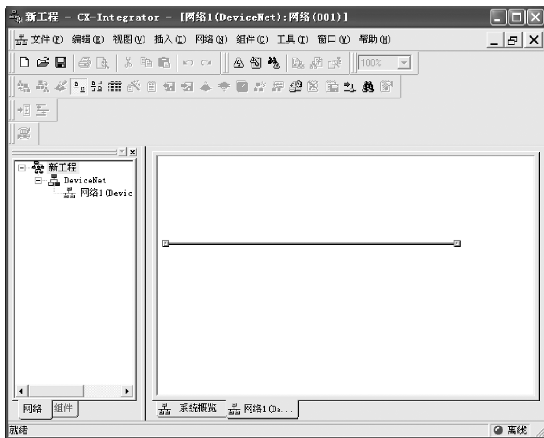


图 4-59　完成网络建立后的主窗口

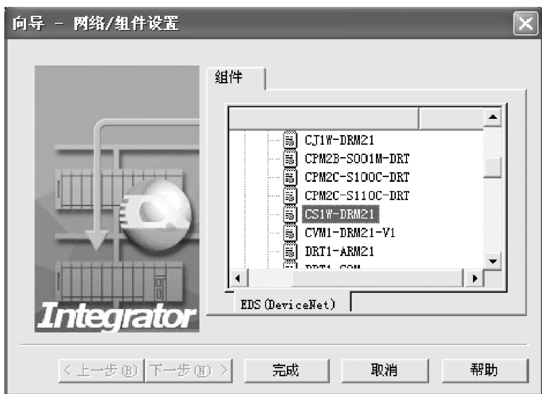


图 4-60　“向导-网络/组建配置”窗口

本例在该窗口上选择“类型（DeviceType）”下及其下“通信适配器（Communications Adaptor）”下的“CS1W-DRM21”。之后点击“完成”。即完成站点 1（作为主站）的插入。本例还有两个从站站点也可照此办法插入。也可如图 4-61 所示，用鼠标从主窗口的左下角拖放所要插入站点到网络上进行插入。该图所示网络已按本例要求插入了各个站点。

3）为注册设备列表。为此，可点击主窗口“组件”主菜单下“参数”项之下的“向导”项。将弹出如图 4-62 所示的设置内存起始字窗口。

可使用缺省值，也可更改。输入输出各有两个区域块，每块 100 字可用。接着可点击“下一步”按钮。将弹出如图 4-63 所示的设置怎样分配 I/O 数据岛 PLC 内存窗口。

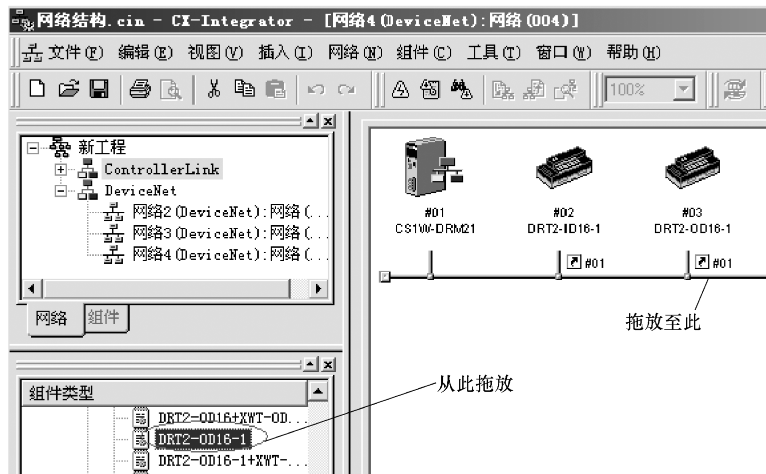


图 4-61　1 个主站 2 个从站网络



图 4-62　设置内存起始字窗口



图 4-63　设置怎样分配 I/O 数据岛 PLC 内存窗口

本例选择“按通道分配每个字”。也可使用“分配以使占用字的总数最小”。后者可两个设备共用一个字，节省 PLC 内存，但不方便。接着再点击“下一步”按钮。将弹出如图 4-64 所示的注册设备窗口。

从图知，这里以完成了注册设备表。此表的含义是，本例主站可管理两个从站，1 个输入从站，用两个字节；1 个输出从站也用两个字节。如果主站不要管理一些从站，如 01 号站，也可点击所选站点，然后点击图示按钮，即可退出该站点到未注册设备列表中。再点击“下一步”将弹出如图 4-65 所示分配结果窗口。

从图可知，这两个点分别在 PLC 中分配有自身的地址。PLC 程序使用这个地址即可进行站点的管理。最后点击“完成”按钮，设置完毕。

之后，当然要存储、联机下载给 PLC，PLC 再重新上电此组态才有效。

（2）主站与小型 PLC 连网

本例配置网络（006）有 2 个站点。如图 4-66 所示。#01 为主站（CJ1W-DRM21），#00 为从站（CPM1A-DRT21）。

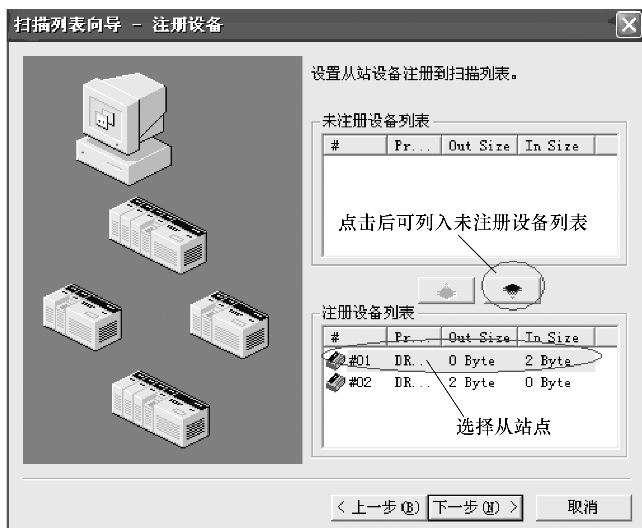


图 4-64　注册设备窗口



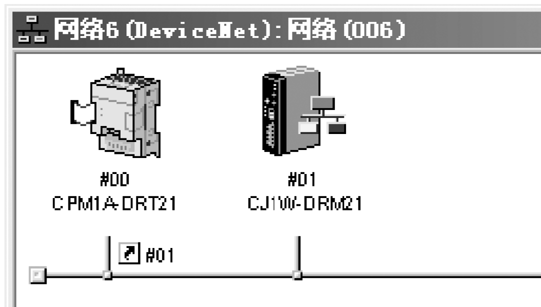


图 4-65　分配结果窗口　　　　图 4-66　CJ1W-DRM21 与 CP1AW-DR21 联网

组网过程与上述 1 个主站 2 个远程 I/O 连网配置相同，不再赘述。以下介绍注册设备表即分配地址。

1）注册设备表。可用上例步骤，也可直接双击图 4-66 主站点图标。之后将弹出如图 4-67所示的编辑设备参数窗口。先在图示通用表单上选择从站，本例为 CPM1A-DRT21。然后点击图示图标，将把该站点列入注册设备表。

2）I/O 分配。点击该窗口 I/O 分配（输出）表单，将出现如图 4-68 所示画面。再点击“自动”按钮。可看到 CPM1A-DR21 4 个输出字节所占 PLC 主站的内存地址为 3200、3201 两个字。

同理点击该窗口 I/O 分配（输出）表单，也可分配 I/O（输出）地址。当然，还有有关表单，还可根据有关要求对从站模块做其他设置。之后，当然要存储、联机下载给 PLC，PLC 再重新上电后，此组态才有效。要注意的是，这里主站 PLC 的输入对应从站为输出，反之也一样。

（3）多主站联网配置实例

有 3 个主站，有 3 个从站。其组态过程与上述 1 个主站、2 个远程 I/O 连网配置相同。本例组成后如图 4-69 所示。



图 4-67 将从站列入主站注册设备表



图 4-68 I/O 分配（输出）表单

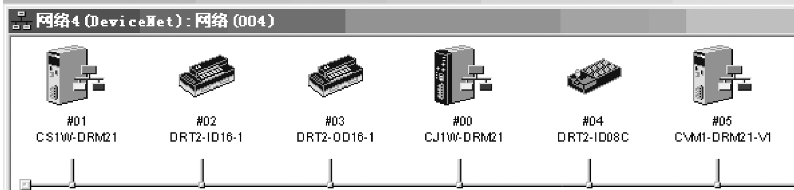


图 4-69 3 个主站 3 个从站

由于有多个主站，所以如果有的主站也要有从站功能时还要对此做设置。如设置#01 主站属性，可用鼠标右键点击该图标，在弹出的下拉菜单上点击“属性”项，将弹出如图 4-70 所示#01 属性窗口。

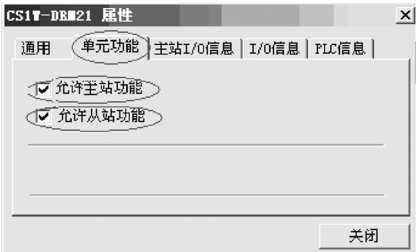


图 4-70 #01 属性窗口

本例在单元功能上，选择器为既允许主站功能，又从允许站功能。意即可作为其他主站的从站，也可作为其他从站的主站。如果只允许从站功能，当然就不能作为主站。本例其他主站无此功能，所以不类似做设置。

之后就是为各个主站列注册设备表。办法同上述 1 个主站 2 个远程 I/O 连网配置实例。如#00 主站，可用鼠标双击它的图标，将弹出如图 4-71 所示的编辑参数窗口。如果要把#01 主站也列入它的注册设备表，选定后点击图示按钮即可。本例按图示操作可把#01 站点作为它的从站。

但如果选的#05 主站点，将告知它没有从站功能，将不能列入本主站的注册设备表。上述组态完成，可点击主窗口上“视图”主菜单下的“详细资料”项，可出现如图 4-72 所示画面。从中可看出这里 3 个主站及其所管理的从站。

之后，当然要存储、联机下载给 PLC，PLC 再重新上电后，此组态才有效。

上述所作配置也可在线进行。硬件设定好了，接线、连网，直接在线扫描，读取各个站点，进而作必要选定。过程可能更简单。



图 4-71 编辑#00 主站参数窗口

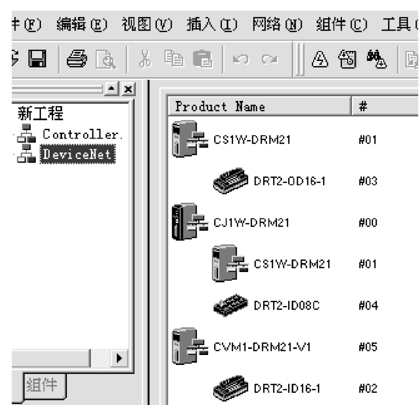


图 4-72 3 个主站及其所管理的从站

4.3.4 三菱 DeviceNet 组件及配置实例

三菱公司 PLC 也有 DeviceNet 模块，如用于 Q 型机的 QJ71DN91，可用作主站，也可做从属主站。其性能见表 4-18 所示。

表 4-18 QJ71DN91 模块性能表

<table>
<tr><th colspan="5">项 目</th><th colspan="6">规 格</th></tr>
<tr><td rowspan="20">通信规格</td><td rowspan="8">用作主站</td><td colspan="3">站点类型</td><td colspan="6">Device 主站</td></tr>
<tr><td colspan="3">可设置站点数</td><td colspan="6">0 ~ 63</td></tr>
<tr><td rowspan="2">可建立连接数</td><td colspan="2">信息连接</td><td colspan="6">63</td></tr>
<tr><td colspan="2">I/O 连接</td><td colspan="6">63(polling, bit strobe, change of state, cyclic)</td></tr>
<tr><td rowspan="4">通信数据量</td><td rowspan="2">I/O 通信</td><td>发送</td><td colspan="6">Max. 4096 points(512 字节)，max. 256 字节每站点</td></tr>
<tr><td>接收</td><td colspan="6">Max. 4096 points(512 字节)，max. 256 字节每站点</td></tr>
<tr><td rowspan="2">信息通信</td><td>发送</td><td colspan="6">Max. 240 字节</td></tr>
<tr><td>接收</td><td colspan="6">Max. 240 字节</td></tr>
<tr><td rowspan="5">用作从站</td><td colspan="3">站点类型</td><td colspan="6">Device 从站</td></tr>
<tr><td colspan="3">可设置站点号</td><td colspan="6">0 ~ 63</td></tr>
<tr><td>可建立连接数</td><td colspan="2">I/O 连接</td><td colspan="6">1(polling)</td></tr>
<tr><td rowspan="2">通信数据量</td><td rowspan="2">I/O 通信</td><td>发送</td><td colspan="6">Max. 1024 点(128 字节)</td></tr>
<tr><td>接收</td><td colspan="6">Max. 1024 点(128 字节)</td></tr>
<tr><td colspan="4">通信速度</td><td colspan="6">从如下选定：125kbps, 250kbps, 500kbps.</td></tr>
<tr><td colspan="4" rowspan="5">最大电缆长度</td><td rowspan="2">通信速度</td><td colspan="3">主干线最大传输距离</td><td colspan="2">下拉长度</td></tr>
<tr><td>粗缆</td><td>粗缆 细缆</td><td></td><td>最大</td><td>总长</td></tr>
<tr><td>125kbaud</td><td>500m</td><td rowspan="3">100m</td><td rowspan="3"></td><td rowspan="3">6m</td><td>156m</td></tr>
<tr><td>250kbaud</td><td>250m</td><td>78m</td></tr>
<tr><td>500kbaud</td><td>100m</td><td>39m</td></tr>
<tr><td colspan="4">网络电流消耗</td><td colspan="6">0. 03A</td></tr>
<tr><td colspan="5">写闪存次数</td><td colspan="6">Max. 100000 次</td></tr>
<tr><td colspan="5">占用 I/O 点数</td><td colspan="6">32 点(I/O 智能 I/O 32 点)</td></tr>
<tr><td colspan="5">5VDC 内部电流消耗</td><td colspan="6">0. 17A</td></tr>
<tr><td colspan="5">重量</td><td colspan="6">0. 11kg</td></tr>
</table>

4.4　ControlNet

关键词：网络更新时间（NUT）、NUT 的时间间隔（NUI）、预定时段、未预定时段、连接标识、连接信息传输、非连接信息传输、信息类产品、扫描器类产品、适配器类产品、数据链接、信息服务、令牌循环周期、发牌周期、对等模式、1：N 模式

ControlNet（控制网）是开放的、工业的、实时控制层网络，可在单一的物理媒体上高速传输 I/O 数据以及消息数据，后者包括上传/下载程序和配置数据、点到点的消息等。ControlNet 提供控制器与输入输出设备、驱动、操作员界面、计算机或其他设备间的连接，并且能整合 AB PLC 的 DH + 网络和远程 I/O 等现存通信方式。

本节将对其做简要介绍，并介绍 AB 公司的 ControlNet 组件、配置实例。同时对 OMRON 的 Controller Link 网络也顺便进行讨论。

4.4.1　ControlNet 简介

1. ControlNet 组成

图 4-73 所示为 ControlNet 一个组成方案。

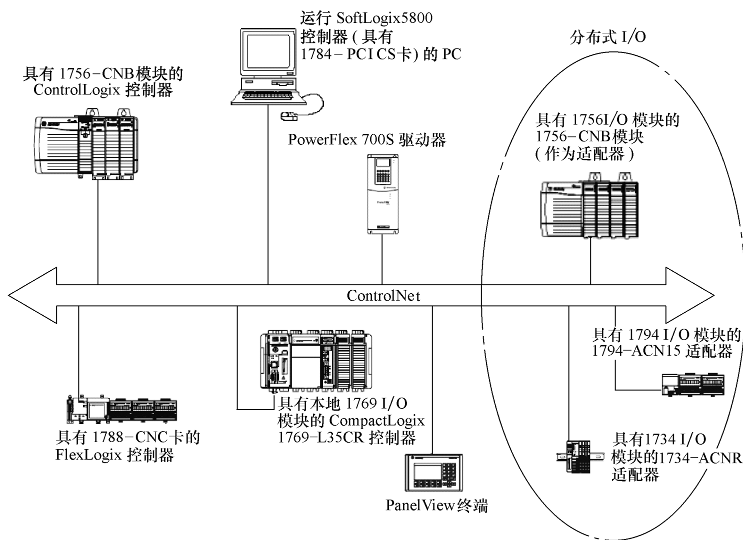


图 4-73　ControlNet 组成方案

从图知，它包含有：控制器、计算机、I/O 模块等。

（1）控制器

配置有 ControlNet 通信模块的控制器，如 AB PLC 公司的 ControlLogix（含 CompactLogix、SoftLogix 等）、ProcessLogix（用于过程控制）、FlexLogix（用于分布式控制）及基于 PC（计算机 + IOLinx 等软件）的控制器。这些控制器可生成生产者和消费者标签（Tag），实时交换数据。还可运用指令，发起用于发送/接收数据或有关配置的通信。

（2）个人计算机

配置有 ControlNet 通信接口的计算机。运用应用软件，可以向控制器上载/下载项目

（含 PLC 程序），可以配置 ControlNet 上的设备，还可以配置网络。此外，配置有 ControlNet 通信口的人机界面（HMI），也有一些类似功能。

（3）基于框架和分布式 I/O 模块

当然在框架或模块上也要配置有 ControlNet 通信接口。有多种适合于 ControlNet 的 I/O 模块，可从中选择适当的 I/O 点数及类型与规格，还有多种如高速计数、热电偶等专用模块。

（4）物理介质

有分接器套件、连接器、电缆（或光缆）、终端电阻及中继器模块（及其适配器，可为中继器提供工作电源）。使用中继器可扩展网络距离，建立不同的拓扑结构及不实现同通信介质的转换。

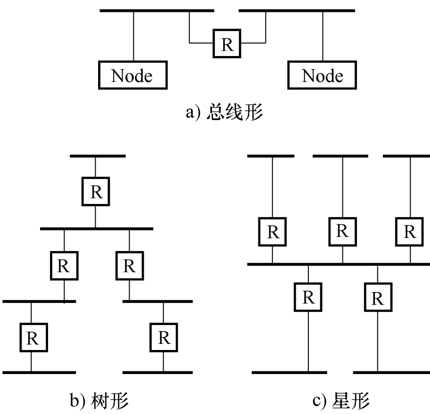


图 4-74　ControlNet 拓扑结构

2. ControlNet 网络结构

对照 OSI 模型，ControlNet 也仅有 4 层。OSI 表示层以上为应用层，或称高层。传输层以下有 3 层，即传输网络层，数据链路层及物理层。

（1）物理层

从使用角度讲，主要是弄清可选择的网络拓扑与物理媒体。可能的拓扑结构如图 4-74 所示。多拓扑及媒体类型还可混合使用。端到端的网络长度变化取决于站点数、媒体类型、中继器的使用。具体见表 4-19 说明。

表 4-19　端到端长度说明

媒体	2 站点	32 站点	48 站点	49 ~ 99 站点
同轴电缆/m	1000	500	250	要求用中继器
光纤	取决于中继器性能、光纤与终端特性			
带中继器同轴电缆或光纤	取决于中继器数量、性能、光纤与终端特性			
最大下拉长度/m	1	1	1	1

当选用同轴电缆做媒体，ControlNet 可用 RG-6 同轴电缆，工业 TV 用的就是这个电缆。此电缆不太贵，并具有高的抗噪声性能。还有若干可利用的接口，以满足各种应用于现场要求。

在网络的每个站点处要配置有分接头（Tap）。接头可用导轨安装，并易于接入主干线电缆。接头有直线的、直角的、“Y” 型的几种类型。尽管这些接头必须在网络不上电时安装，但它允许网络上电时站点的加入或移出。接头可沿主干线电缆安装在任何地方，但要大于站点间最小的要求距离。标准的站点接线是由接头下拉 1m。每个站点可利用变换器耦合提供电气绝缘。

当选用光纤媒体，ControlNet 可通过成对地安装在光缆端的发送器、接收器组成全双工的、点到点的连接。光缆特性见表 4-20。

表 4-20 光缆特性

规　　格	短距离(300m)	中距离(3000m)
光纤技术	Step index, hard clad Silica(HCS)	Graded index, multi-mode
Core/Cladding	200/230μm	62.5/125μm
Numerical Aperture	0.5	0.275

也可选择冗余电缆媒体。它允许全部信息同步在两个电缆上传送。每个站点评估信号质量，并动态选用最佳质量的信号。

除了用于控制与信息处理的 ControlNet 接口之外，每个 ControlNet 站点还都有一个访问口（Network Access Port，NAP），为计算机或其他支持工具接入网络与其他网络站点通信提供可能。网络访问口使用的是标准 8 针 RJ-45 连接器。

可使用中继器增加网络端到端长度及每段的站点数。中继器还可用于使电缆接入光缆，以抗噪声干扰及增加传送距离。对给定系统，最多中继器数受由中继器引起传送延迟的限制。在确定系统的最多中继器数及最大传输距离时，须计算网络中两个最远的站点间的一个个延时（媒体、分接口及中继器）的总和，其值必须小于 120μs。

（2）数据链路层

站点访问网络取决于时间。每个站点仅仅在所分配的时间段才可访问介质、发送数据。这种机制称为并发时间域多重访问（CTDMA，Concurrent Time Domain Multiple Access）。其基础是选定好网络更新时间（Network Update Time，NUT）。这 NUT 的时间间隔（Network Update Interval，NUI）配置好后是固定的，并周期重复着。这里，NUI 代表着 ControlNet 网络上预定数据传输的最快更新速率。例如，以 5ms 的 NUI 运行的网络无法以快于 5ms 的速率发送数据。图 4-75 所示为 NUT 的示意。

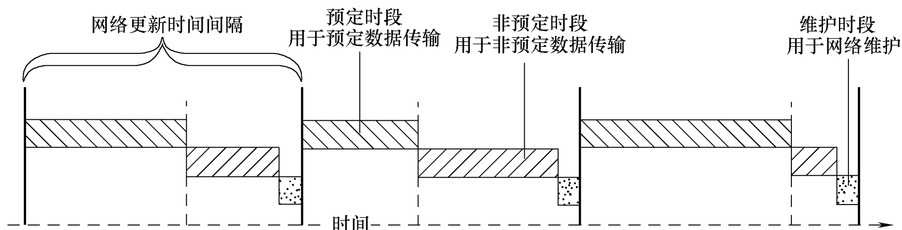


图 4-75　网络更新时间示意

这里，每个 NUI 分都为 3 个时段。

1）预定时段：如图 4-76 所示，在此时段，各站点按地址编号从低到高访问媒体一小段时间，确保上述生产者和消费者标签数据（远程 I/O 及模拟量数据及点对点的互锁数据）的都得以实时传输。ControlNet 数据传输的确定性、实时性就是有了这个时段才得以保证。

这里，好像也有一个隐含令牌在站点间传输，但实际上当然没有了。它的各个站点只是根据自身地址由时间确定访问权。在同一时间，也只允许一个站点有这个访问权。不是自己的访问时间，站点要不在监听，要不在等待不在线站点是否确实不在线（需要一个跟踪时间，Slot Time，网络站点地址不连续时将出现此情况）。这跟踪时间的长短取决于网络覆盖长度及使用的中继器的数量，约为 0.025ms。

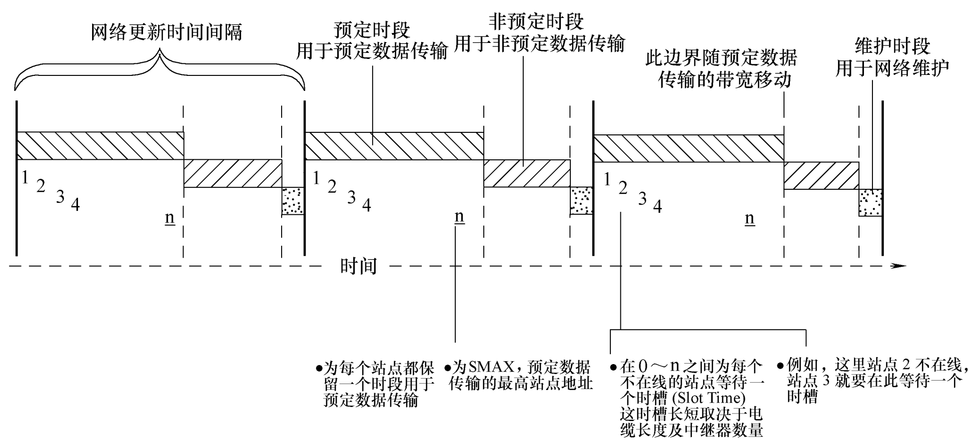


图4-76　网络更新时间示意

提示：站点最好为连续编号，已减少等待时间。预定时段不为地址大过SMAX的站点分配访问权。所以，SMAX的设定要能覆盖要求使用预定时段所有站点。

2）未预定时段：它分配访问权也是按地址顺序轮流。一个站点可以有1、2或多次机会获得访问权，但不保证各站点都能获得。同时，它的地址轮流是在0到UMAX之间进行。而UMAX为所有可能配置最高站址，比SMAX要大，缺省为SMAX+8。图4-77所示为非预定时段站点访问的示意。

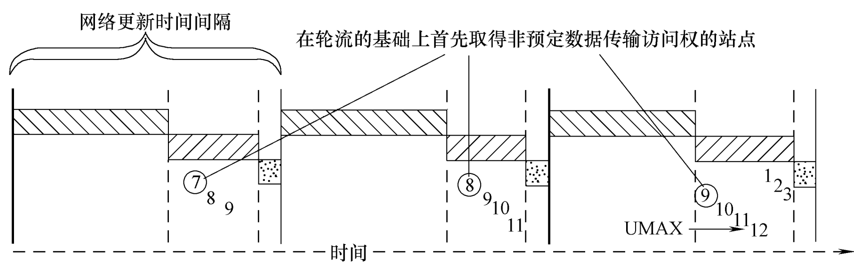


图4-77　非预定时段站点访问的示意

从图知，这里网络访问权也是各个站点也是轮流，但每NUI分配到的只是部分站点。如图先是7、8、9，接着为8、9、10、11（不管8、9在上一时段是否完成），再为9、10、11、12（12为UMAX，不管9、10、11在上一时段是否完成）。这里首次可访问的站点是轮流递增的。但这不意味着一定为它所用，只是为它的使用提供优先权。它不用依次留给下一个站点用。

由于各站点在非预定时段访问权是不确定的，所以它只用于没有严格时间限制的数据传输。如：建立连接传输；点对点信息数据传输；程序的上载与下载等。

3）维护：是NUI的最后部分。用作网络维护。在此时段，称为仲裁器（moderator，所连接的MAC ID站址最小站点）的站点把仲裁帧广播传送给各个站点，以保持各站点的网络参数（如UNI、SMAX、UMAX及前述网络跟踪时间）一致及定时器同步。与NUT的预定和未预定部分的时间相比，网络维护所需的时间很短。它只需传送125字节数据，约占0.2毫秒。尽管它占的时间短，但很重要。因为ControlNet与CompoNet一样，是基于时间控制。

所以，不仅各个站点要有准确的定时器，而且，各个站点的定时器还必须保持同步。否则网络访问的冲突将是不可避免的。

用户可使用网络配置工具选择 NUI 等参数。这些参数可保存在站址最低的站点或其他备用站点上。如最低站址出现故障，则次最低站点将接替网络维护。

提示：ControlNet 每个站点的接口芯片（ASIC）都有作为仲裁器（moderator 或称 Keeper）的能力。最低地址站点如果出现故障，则次次最低站点将接替实现它的仲裁功能。

从上分析可知，这里的关键是确定 UTI。其最小值除了应保证预定时段所有站点预定数据及维护时段仲裁器维护数据（125 字节）发送外，还要给非预定时段保留一定时间，至少有一个站点能发送可能最大长度为 510 字节的数据。已知 ControlNet 网络的波特率为 5Mbit/s，由此当然可计算出最小 NUI 数值。实际当然不必这样具体计算，多可运用相关网络配置软件处理。只是也从此可知，它的预定数据传输量，即于此有关的连接数，也是受限制的。

链路层另一问题是数据帧的组织。其媒体访问控制帧［Media Access Control（MAC）frames］格式如图 4-78 所示。

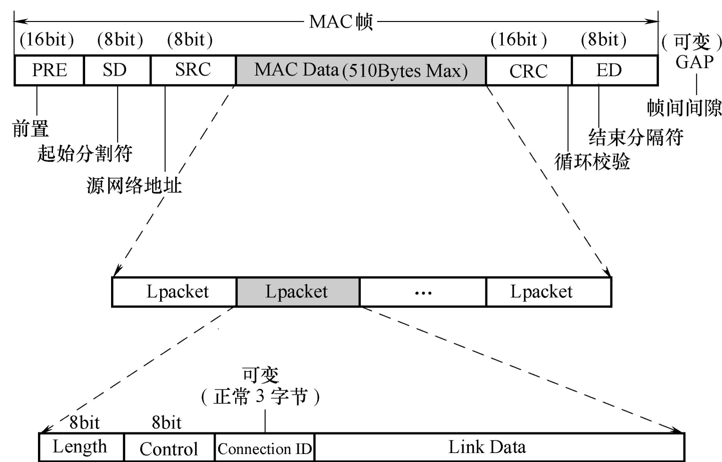


图 4-78　ControlNet 帧格式

这里一个 MAC 帧为一组打包数据。其中可能含有多个链接数据包（Link packets）。这链接数据包是指站点设定的标签数据。从图知，MAC 帧先是帧 PRE（先导），接着为起始界定符（SD），再就是源站点地址（SRC），然后是 MAC 数据（一个个链接数据包），再后为 CRC 校验码，最后结束界定符。帧之间有当然也要留有间隙。至于链接数据包的格式如图 4-79 所示。

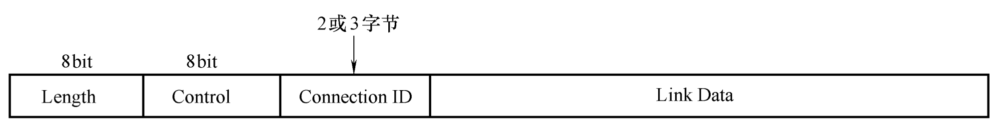


图 4-79　链接数据包帧格式

它有帧长度字节、控制字节、连接标识（connection ID，CID）及标签数据 4 部分组成。这里 CID 是在标签数据配置是自动生成的，提供其他站点判断这组标签是否为其所需。CID

有两种格式：固定连接格式，占 2 个字节，记录服务编码及目标地址；通用连接格式，占 3 个字节，记录唯一的特定连接 ID。

（3）传输网路层

ControlNet 使用两种信息传输格式：

1）非连接信息传输。用于建立连接过程及传送不常用的、低优先级的信息。它常使用上述非预定时段，在站点中，其资源被称为未连接管理器（UCMM）。符合标准的 ControlNet 产品接收其他站点的要求时，应使 UCMM 使能。

2）连接信息传输。在 ControlNet 上，每个站点的资源优先用于诸如显式信息传输和实时的 I/O 数据传输。具体可通过 UCMM 予以保留或配置，以用于有关通信服务。

打开连接的过程称连接开始，发起连接的站点称连接源，简称源。相反，响应连接要求的站点称连接目标，简称目标。

ControlNet 有两种信息传输连接：显式和隐式（I/O 数据）。显式信息传输连接是点对点的关系，它的建立适合两站点间的请求/响应的信息传输。在性质上讲，这些连接是通用的，可用于访问站点任意可访问项。显式信息传输使用的是上述 NUI 的非预定时段。

相反，隐式信息传输连接则用于在规定的时间间隔内，重复传输用户的指定 I/O 数据。在性质上讲，它是多播的。常设为 1 对多的关系，目的是用好生产者/消费者关系的潜力。隐式信息传输使用的是上述 NUT 的预定时段，以确保数据传输的确定性。

ControlNet 支持 3 类网络通信能力的产品：信息类，适配器类及扫描器类。每类支持一组基本的通信服务，但也可选用其他服务。

信息类产品：支持非计划的显式信息传输（连接和非连接），这信息为其他类产品所发送或接收。信息类产品是显式信息连接要求的目标；同时也是这些要求的源。但它不能在 NUT 预定时段发送或接收实时 I/O 数据。

这些类产品包括：

用于程序上载和下载到 HMI、机器人和 PLC 的计算机接口卡；

用于支持 HMI 采集控制系统数据应用程序的计算机接口卡或其他硬件；

不要求实时 I/O 响应的软件应用；

网络配置与诊断工具。

适配器类产品：是扫描器类产品计划 I/O 数据连接要求的目标。它不能发送或接收预定时段的 I/O 数据，除非扫描类产品要求它这么做。它不能预定存储或生成数据。适配器类产品可接受来自全部其他类产品的非预定显式传送要求（连接和非连接）。也可用非预定信息传送与任意类的产品交换数据（点对点），但不能要求发起这个关系。

这些类产品包括：

生产和消费实时预定数据的 I/O 机架适配器；

根据 PLC 或其他控制器要求，发送和接收实时预定数据的磅秤、焊接机、驱动器和机器人；

与计算机接口卡、PLC 相互发送和接收非预定数据的磅秤、焊接机、驱动器和机器人；

与 PLC 之间发送和接收预定和非预定数据的 HMI。

扫描类产品：是要求与适配器类产品预定 I/O 数据连接的源，也是要求与其他扫描器类产品非预定点对点连接的源头。也可能是来自其他类产品非预定显式连接要求的源或目标。

也能向或从全部其他类产品发送或接收非预定信息。

这些类产品包括：

可与 I/O 机架适配器、PLC、机器人、磅秤、焊接机和 HMI 产品发送和接收计预定实时数据的 PLC、控制器和机器人；

可与其他 PLC、机器人、磅秤、计算机插卡、焊接机和 HMI 产品发送和接收非预定数据的 PLC、控制器和机器人；

用于基于计算机控制的计算机接口卡。

（4）应用层

也是高层。与 CompoNet、DeviceNet 一样也是用严格面向对象的 CIP 协议。具体不再赘述。

3. ControlNet 拓扑结构

ControlNet 网络支持多种拓扑结构。最简单的形式是一个干线，可使用分接头和 1m 的支线向其中连接站点，如图 4-80a 所示。如使用中继器可创建其他拓扑，如图 4-80b 所示为星形结构，再如图 4-80c 所示为环形结构。同轴电缆中继器通常用在干线和星形拓扑中。光纤介质可用在干线和星形拓扑结构中，它也是实现环形冗余的唯一方法。

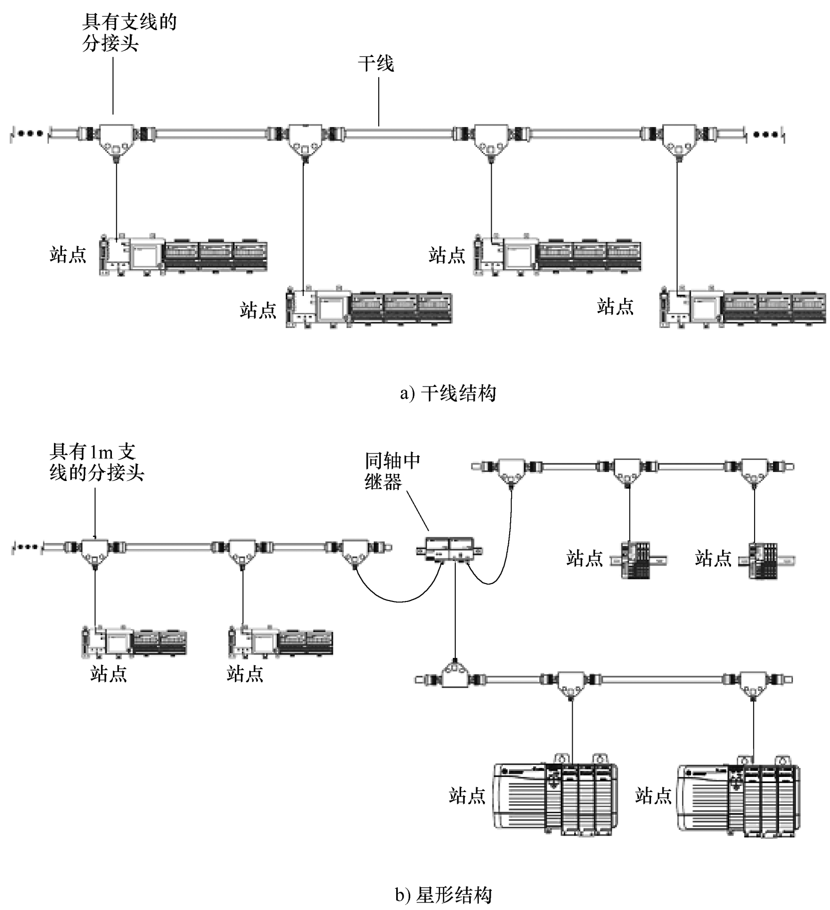


图 4-80　ControlNet 拓扑结构示例

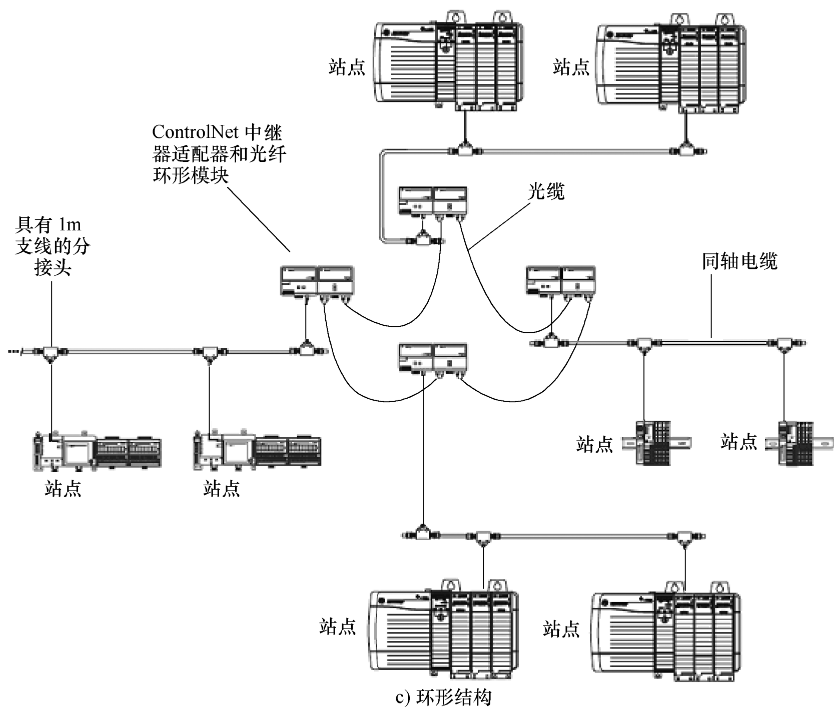


图 4-80　ControlNet 拓扑结构示例（续）

在 ControlNet 网络中，最大距离取决于分段中的站点数。分段是指两个终结器（终端电阻）之间的主干部分。使用中继器可添加更多分段或延长距离。在 ControlNet 中，只有两个分接头时，分段最大距离为 1000m。而每增加一个分接头，最大距离要减少 16.3m。下式可用以计算最大分段距离：

允许的最大分段长度 = 1000m(3280ft) − 16.3m(53.4ft) × [分接头数 − 2]

如果允许最大距离不符要求，则要增加中继器。可用图 4-81 确定是否需要中继器（假定使用 1786-RG6）。

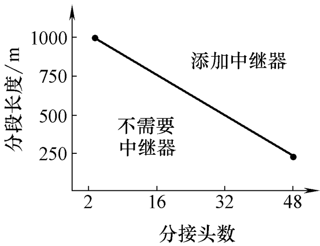


图 4-81　确定是否需要中继器简图

4. ControlNet 规格

ControlNet 规格见表 4-21 所示。

表 4-21　ControlNet 规格

性能指标	ControlNet	最大帧长	510 字节
拓扑结构	星形、树形、总线形	仲裁方式	并发时间域多路存取（CTDMA）
通信速率	5Mbit/s		
最多节点	99 个	通信方式	主/从，多主，对等
最大无中继距离	同轴：5km 光纤：30km	主要数据交换方式	生产者/消费者
总线冗余	可		

5. ControlNet 特点

1）使用生产者/消费者网络模式读写基于 Logix 的系统中的预定数据，而不是使用传统

的源/目标（主/从）模式。使用传统模式，控制器靠轮询输入模块以获取其输入状态。而使用生产者/消费者网络模式，控制器不要去轮询数字输入模块，相反，输入模块会在发生状态变化（COS）时或定期生成（多路广播）其数据。更新的频率取决于配置期间选择的选项以及输入模块在网络中的位置。因此，输入模块是输入数据的生成者，而控制器是数据的使用者。控制器还可以生成由其他控制器使用的数据。

使用生成者/使用者网络模型可降低网络流量，提高传输速率，可最大限度地优化了带宽的利用率和便于控制信息的同步；同时还可以在 ControlNet 和 DeviceNet 或 EtherNet/IP 上的设备之间进行通信，而无需额外编写应用程序代码。无需在桥接模块中配置路由表，这大大简化了维护和模块的更换。

2）ControlNet 是大覆盖范围（用光缆最大距离为 30km、用同轴电缆加中继器可达 6km）高数据吞吐量（最大帧可达 510 字节）、高传输速度（5Mbit/s）、多站点（最多可达 99 个站点）的控制和 I/O 网络，可构成多主、主/从、对等的通信结构。媒体访问算法可确保控制信息传送时间的准确性、确定性。可利用预定功能传输时效性强的控制信息（即 I/O 数据和控制联锁），实时处理大量 I/O 数据。还可利用未预定数据的传输方式，传输其他信息（即时效性不强的消息，如程序上载和下载）。而且这些其他信息传输也不会干扰时效性强的消息传输。

3）灵活的拓扑结构（总线形、树形、星形等），简单且灵活的安装方式可供选择。

4）站点可在线接入与移出，可以从任何一个站点访问整个网络，给 PLC 编程及诊断，实现网络存取。网络配置、维护简单。

5）具有灵活的安装选择，网络介质可选用铜、光纤、光纤环、冗余介质、本安材料可使用各种标准的低价同轴电缆，也可使用具有强抗干扰性和本征安全性的光纤，多种介质选择（同轴电缆、光纤和其他）。

6）冗余并支持媒体冗余方式。正是 ControlNet 的这些特点 AB 公司才把它作为如下应用。即：作为 ControlLogix 平台的缺省网络；作为远程 I/O（RIO）网络的代替网络；作为多个分布式 DeviceNet 网络的骨干网；作为对等连锁网络；代替 AB 公司使用多年的 Data Highway Plus 网络。

4.4.2 AB ControlNet 组件及配置实例

1. AB ControlNet 组件

上述介绍 ControlNet 组成中的产品，AB 公司均有提供。主要有信息类、适配器类、扫描器类产品。此外还有通信介质及其有关产品。

（1）ControlNet 通信模块

有的用作扫描器、消息桥接器，有的可用作适配器。针对 Logix5000 系列 PLC，AB 公司提供的 ControlNet 通信模块及其应用见表 4-22 所示。

上述模块的特性有：支持消息传递、生产者/消费者标签和分布式 I/O；与 DeviceNet 和 EtherNet/IP 共享相同的应用层；通过 RG-6 同轴电缆或 200/230 微米 HCS（硬覆层石英）光纤电缆进行对接；无需路由表可实现 CIP 网络路由；支持使用同轴电缆和光纤中继器以便进行隔离和延长传输距离。

表 4-22　Logix5000 系列 PLC ControlNet 通信模块

ControlNet 模块：	用作 I/O 桥接器①	用作消息桥接器②	用作 I/O 适配器④
1756-CNB 1756-CNBR(冗余)	×	×	×
1769-L32C、1769-L35CR	×	×③	
1788-CNC(同轴电缆)、1788-CNCR(同轴电缆冗余)、1788-CNF(光纤) 1788-CNFR(光纤;冗余)	×	×	
1794-ACN15、1794-ACNR15			×
1797-ACNR15			×
1734-ACNR			×

① 模块用作 I/O 桥接器（即扫描器）时，模块可以（与控制器协同工作）向远程 I/O 发起连接。
② 模块用作消息桥接器时，模块可以充当从一个网络到另一个网络或背板的网关，而无需控制器程序。要启用 1784-PCC 卡的网关功能，RSLinx Gateway 是必需的。
③ 如果 CompactLogix 1769-L32C 或 1769-L35CR 控制器用作从 ControlNet 到 DeviceNet 的桥接器，则必须在本地底盘中使用 1769-SDN 模块。
④ 模块用作 I/O 适配器时，模块可与 I/O 进行对接，还可充当从控制器发起的远程 I/O 连接的目标。

（2）扫描器用的控制器产品

ControlNet 通信模块与其结合后成为网络的扫描器。控制器就是各种 AB PLC 的 CPU。当今其主流产品为 Logix5000。具体见表 4-23 所示。

表 4-23　ControlNet 的 Logix5000 主流产品

特　　点	FlexLogix	ControlLogix
内存(最大) 1 字 =10 Logix 字节	512K 字节	8M 字节
I/O(最大)	512 点(数字量) 或 128 点(模拟量), 或者是二者的混合	最多 128000 点(数字量)或 3800 点(模拟量),或者是二者的混合
Local I/O	1794 FLEX I/O 1797 FLEX Ex I/O	1756 I/O
ControlNet 网络 I/O	1734 POINT I/O 1756 I/O 1771 I/O 1794 FLEX I/O 1797 FLEX Ex I/O	1734 POINT I/O 1756 I/O 1771 I/O 1794 FLEX I/O 1797 FLEX Ex I/O
控制器冗余热备	有,通过 DeviceNet 扩展 I/O	有,通过 ControlNet 扩展 I/O
编程软件	RSLogix 5000	RSLogix 5000
编程语言	梯形图,FBD(功能块图),SFC(顺序功能图),ST(结构文本)	梯形图,FBD(功能块图),SFC(顺序功能图),ST(结构文本)
接口需求	1788-CNC(同轴电缆) 1788-CNCR(同轴电缆冗余) 1788-CNF(光纤) 1788-CNFR(光纤,冗余)	1756-CNB 1756-CNBR(冗余)

（3）信息类产品

主要是配置有 ControlNet 接口卡、转换器及相应软件的计算机、人机界面。有多种总线插卡、转换器。用它可使计算机接入 ControlNet 网络。再通过 AB 提供的网络软件即可进行网络通信、监视、组态及 PLC 编程。这些接口的选用见表 4-24 所示。

表 4-24 AB ControlNet 接口卡选用表

如果用户计算机	选　择	型　号	技 术 指 标
有 PCMCLA 插槽,并且要进行编程,监视或组态网络,以及维护和故障诊断	ControlNet PCMCLA 通信接口卡 网络接入电缆	1784-PCC 1784-PCC1	• 支持 31 条非预定时间连接 • 在 Windows 95/98/ME/NT/2000/XP 环境下驱动
具有 5V PCL 插槽,并且要执行非预定时间通信、编程、监视或组态网络,以及通过 SoftLogix5800 控制器进行维护或故障诊断	ControlNet PCL 通信接口卡	1784-PCLC	• 支持 128 条非预定时间连接 • 在 Windows 98/ME/NT/2000 环境下驱动
具有 5V PCL 插槽,并且要执行预定或非预定时间通信、编程、监视或组态网络,以及维护、故障诊断或通过 SoftLogix5800 控制器控制 I/O	ControlNet PCL 总线 I/O 卡	1784-PCLCS	• 支持 128 条非预定时间和 127 条预定时间连接 • 在 Windows NT/2000/XP 环境下驱动
使用 ISA/ELSA 总线接口,并且想要将应用连接到任意 ControlNet 网络,执行非预定时间通信在线,或组态网络	ControlNet LSA 总线接口卡	1784-KTCX15	• 支持 25 条非预定时间连接 • 在 Windows 95/98/ME/NT/2000/XP 环境下驱动
使用 ISA/ELSA 总线接口,并且要执行预定时间通信或者通过 SoftLogix5 控制器控制 ControlNet I/O,或者通过应用如 C++或 Visual Basic 控制 ControlNet I/O	ControlNet LSA 总线扫描器卡	1784-KTCS①	• 支持 127 条预定时间连接 • 在 Windows NT/2000 环境下驱动 • 使用 LOLinx 软件开发工具作为软件(如 SoftLogix,客户 Visual Basic 程序,以及客户 Visual C++程序)的 I/O 应用接口
具有一个串口,想通过它将设备连接到 ControlNet 网络上	ControlNet 通信模块	1770-KFC15 或 1770-KFCD15 或 1747-KFC15	• 要求一个 115/230V 交流电源 • 要求一个 24V 直流电源(1770-KFCD15) • 电力来自 SLC 机架背板(1747-KFC15) • 支持 14 条连接(1770-KFC15) • 支持 32 条连接(1747-KFC15) • 在 Windows 95/98/NT/2000/XP 环境下驱动

① 该模块是一个扫描器(即该模块可以向远程 I/O 发起连接)。

(4)适配器用的分布式模块化 I/O 产品

ControlNet 通信模块或接口与分布式模块化 I/O 及基于机架 I/O 结合将成为网络的适配器。这里基于机架 I/O 与当地使用的没有区别。分布式模块化 I/O 及其配套的适配器见表 4-25。

表 4-25 AB 分布式模块化 I/O 及其配套的适配器

I/O 模块	选择适配器	技 术 指 标
1734 POLNT I/O	1734-ACNR(冗余)	• 高度模块化(可混合,与用户的精确需求匹配) • 可拆卸端子块 • 具有带电插拔(RIUP)的特点 • 易于分散 • 全范围的数字量、模拟量、专用、以及温度模块 • 可达 252 点/适配器

（续）

I/O模块	选择适配器	技术指标
1794 FLEX I/O	1794-ACN15 1794-ACNR15(冗余)	• 独立于端子块基座的模块 • 具有带电插拔(RIUP)的特点 • 24/48V 直流 • 120/230V AC • 继电器输出、模拟量、温度、专用、计数器及系列模块 • 2-32点/模块
1797 FLEX Ex I/O	1797-ACNR15(冗余) 1794-ACN15 * 1794-ACNR15 * * 在防爆场合配用1797-BIC和1797-CEC 基于机架的I/O	• 用在防爆场合的具有本征安全性的I/O • 独立于端子块基座的模块 • 具有带电插拔(RIUP)的特点 • 数字式(NAMUR)模拟量,温度、频率 • 2~16点/模块
1746 I/O	1747-ACN 1747-ACNR(冗余)	• 模块化、高密度I/O • 24V交流/直流 • 120V交流/直流 • 240V交流 • TTL、模拟量、温度、组合、快速、继电器和许多专用模块 • 4~32点
1756 ControlLogix I/O	1756-CNB 1756-CNBR(冗余)	• 高级诊断和快速升级 • 模拟量和离散量I/O • 具有带电插拔(RIUP)的特点 • 操作向导简化I/O组态 • 5/24/48/125V直流 • 120/240V交流 • 模拟量、专用和运动控制接口 • 4~32点
1771 I/O	1771-ACN15 1771-ACNR15(冗余)	• I/O可选择范围最宽 • 24V • 120V • TTL、模拟量、温度、高速、专用和组合模块 • 4~32点

此外还有其他适配器产品。如配置有ControlNet接口的变频器。品种规格也很多，具体略。

（5）通信介质。有分接器套件、连接器、电缆及附件。中继器模块及其适配器（提供中继器电源）。表4-26所示为AB的相关组件。

表4-26 AB通信介质等相关组件

如果想要	选择	型号	技术指标
在ControlNet网络中进行IP20 BNC连接	ControlNet同轴电缆分接器套件 直角T型分接器 直线T型分接器 直角Y型分接器 直线Y型分接器	 1786-TPR 1786-TPS 1786-TPYR 1786-TPYS	振动/冲击2.5g
	ControlNet同轴电缆连接器 套型连接器,插头对插头 BNC,插头 锥形连接器,插孔对插孔 Isolated Bulkhead隔离式堵塞连接器,插孔-对-插孔 终结器,插头 分接器虚拟负载 跳线,插头对插头(长5in)	 1786-BNCP 1786-BNC 1786-BNCJ 1786-BNCJl 1786-XT 1786-TCAP 1786-TJPR	

（续）

如果想要	选　　择	型　　号	技术指标
ControlNet 网段使用铜质同轴电缆	用于 BNC 和 TNC 的 ControlNet RG-6 四芯屏蔽同轴电缆 高柔性(304.8m[1000ft.]) 标准 PVC CM-CL2（304.8m[1000ft.]） 同轴电缆工具套件	 1786-RG6F/A 1786-RG6 1786-CTK	10MHz/1000ft 下衰减 13.5dB 10MHz/1000ft 下衰减 5.99dB
在 ControlNet 网络中进行防水(IP67),耐恶劣环境的 TNC 连接	带可拆卸分支电缆 ControlNet IP67 分接器套件 套型连接器,插孔对插头 TNC,插头 锥形连接器,插孔对插孔 Isolated Bulkhead 隔离式堵塞连接器 Isolated Bulkhead 隔离式堵塞连接器 插孔对插孔,TNC 到 BNC 终结器,插头	 1786-TCT2BD1 1786-TNCLP4 1786-TNC-L10 1786-TNCJ4 1786-TNCJ14 1786-BNC2TNC 1786-TNCLXT4	振动/冲击 10g
带 V 型针式连接器的预制短距离光纤介质	ControlNet 短距离光缆 10m 电缆组件 20m 电缆组件 60m 电缆组件 100m 电缆组件 200m 电缆组件 300m 电缆组件	 1786-FS10 1786-FS20 1786-FS60 1786-FS100 1786-FS200 1786-FS300	只能和 1786-RPFS 一起使用 对于 1786-RPFM, – RPFRL 和 RPFRXL,请咨询当地光缆供应商
在防爆场合连接设备到 ControlNet 网络	具有本征安全性的 ControlNet(FLEX Ex)分接器套件 FLEX Ex 直角 T 型分接器 FLEX Ex 直线 T 型分接器 FLEX Ex 直角 T 型分接器 FLEX Ex 直线 Y 型分接器	 1797-TPR 1797-TPS 1797-TPYR 1797-TPYS	与 1797-ACNR15 一起使用
	具有本征安全性的 ControlNet (FLEX Ex)连接器 FLEX Ex 终结器 FLEX Ex 安全分接器虚拟负载	 1797-XT 1797-TCAP	
	具有本征安全性的 ControlNet (FLEX Ex)附件 FLEX Ex Boot 绝缘配件 FLEX Ex 电缆标记配件	 1797-BOOT 1797-EXMK	
对 ControlNet 网段进行防爆区域和非防爆区域之间的隔离	ControlNet 同轴电缆安全隔离器(Barrier)	1797-BCNR	也可选择光纤中继器模块 1786-RPA 和 1786-RPFM 到 1797-RPA 和 1797-RPFM
从膝上型计算机连接到 ControlNet 网络	ControlNetwork Access Cable 网络接入电缆(3.05m,10ft.)	1786-CP	和所有列在表 3.5 内的 ControlNet PC 接口一起使用(不包括 1784-PCC 卡)

（6）相关软件

主要是 AB Logix5000 系列 PLC 编程软件，RSLinx 网络软件及 RSNetwork for ControlNet 网络配置与监控软件。

2. AB ControlNet 配置及其实例

AB 公司的 Logix5000 系列 PLC 与其他 PLC 重要不同是，除了与具体输入、输出有关的

数据外，它没有像 OMRON PLC DM 等那样内部器件。它只有数据区。用户可根据自己需要，在这个数据区中，定义各种类型的数据。甚至于用户还可自己定义所需要的数据类型。所以，它的通信模块也不像其他 PLC 通信模块那样有专用于通信的、功能明确的缓冲区，而只有内存区。用户使用时也要根据需要定义。这个定义的形式就是 AB PLC 的标签（Tag）。有关这些标签定义将在以下几个实例一并予以说明。

（1）计算机接入 ControlNet 网络配置实例

目的是实现计算机与 PLC 通信。上下载 PLC 设定、程序，以及对 PLC 监控。图 4-82 所示为计算机与 AB PLC 网络可能的连接。

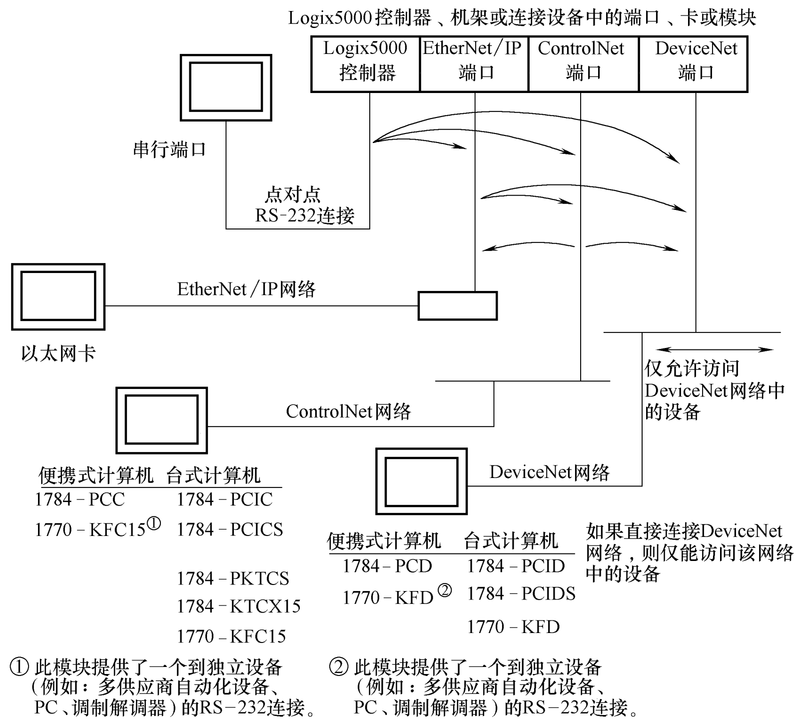


图 4-82　计算机与 AB PLC 网络可能的连接

从图知：计算机可通过多种接口与 PLC 物理连接。具体有：用串口连接；用以太网卡与 PLC EtherNet/IP 端口连接；用 ControlNet 网卡与 PLC ControlNet 端口连接；用 DeviceNet 网卡与 PLC DeviceNet 端口连接。有了这些连接即可使计算机接入 PLC 的上述不同网络。

AB Logix5000 系列 PLC 还有一个重要特点是，它的机架背板不仅有总线，还有专用管理模块之间通信的 CPU。这样，在它的机架上，各模块，如 CPU 模块（每个机架可安装多达 4 个 CPU 模块）、通信模块等，之间的数据交换可自动实现。AB 公司还提供 RSLinx 这类网络软件。运行它不仅可激活上述计算机网卡驱动，还可不必设置路由表，使用上述硬件配置，也可实现如图所示的各网络间的路由。这就是常说的 AB NetLinx 网络架构独到之处。本例使用的 ControlNet 网卡，其具体激活步骤为

1）运行 RSLinx 软件，如图 4-83 所示，选择 Configure Driver（配置驱动程序）项。

2）为 ControlNet 设备选择驱动程序。如图 4-84 所示，在本例中，这里选择 1784-PCICS 卡。还可以通过 1784-PCC 卡将计算机与 ControlNet 网络连接。

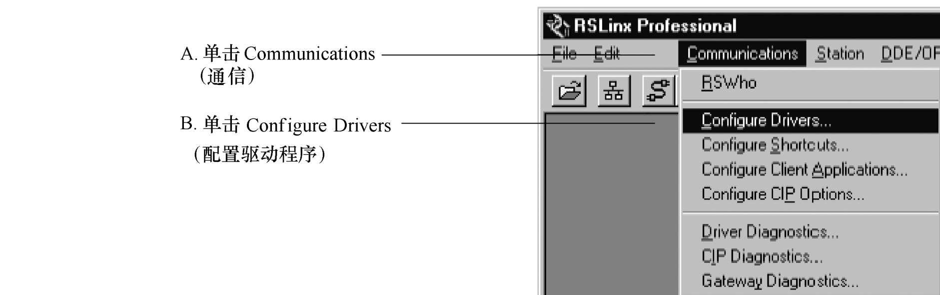


图 4-83 运行 RSLinx 软件

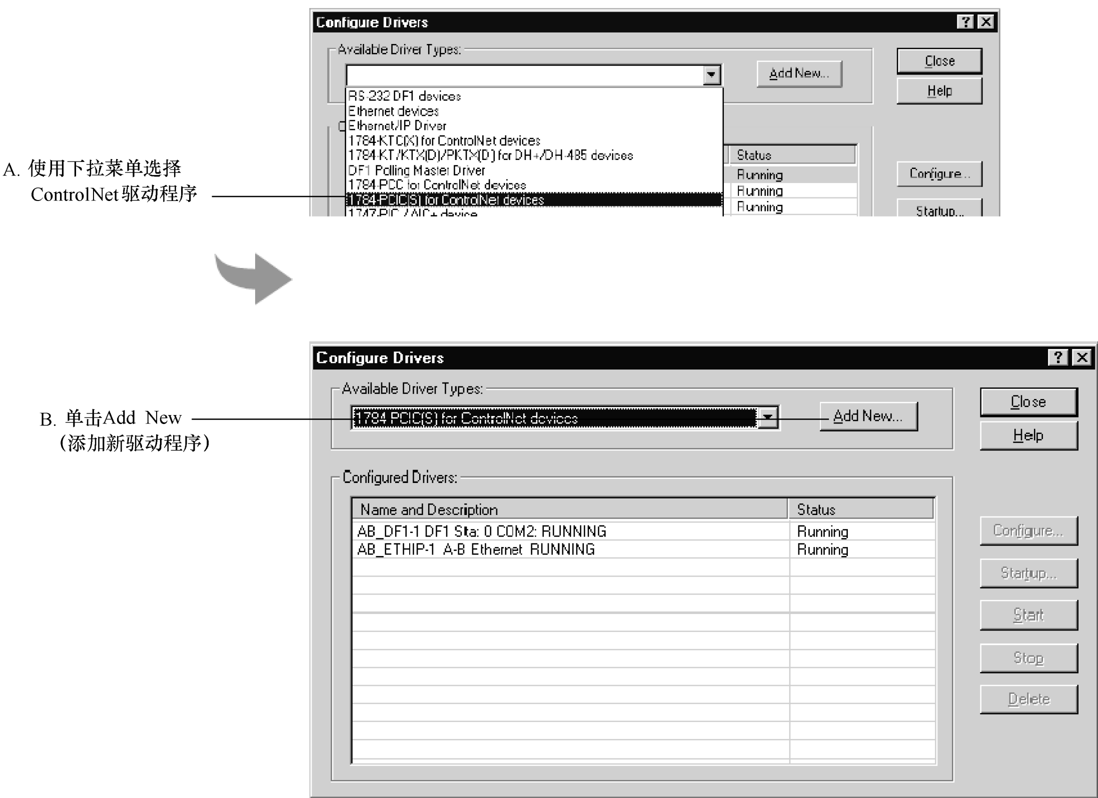


图 4-84 为 ControlNet 设备选择驱动程序

3）命名 ControlNet 驱动程序。如图 4-85 所示，命名其为 AB_PCIC-1。

4）创建驱动程序后，如图 4-86 所示步骤在进一步配置。只是要注意这个配置应与计算机内的 ControlNet 模块相对应。

这时，驱动器处于可用状态，可运行 RSLogix 5000 编程软件的 Who Active（活动项）中，选择 ControlNet 端口，即可与 PLC 联机、通信，进而可运用 RSLogix 5000 编程软件上下载 PLC 项目（设置及程序等）。或运行 RSNetWorx 软件预定 ControlNet 网络。或操作 HMI 类型应用程序。事实上，计算机接入 ControlNet 网络主要功能也就是这些。

（2）用于远程 I/O 控制的配置

在此例中，Logix5000 控制器用本地机架中的 ControlNet 通信模块，作为扫描器连接 Con-

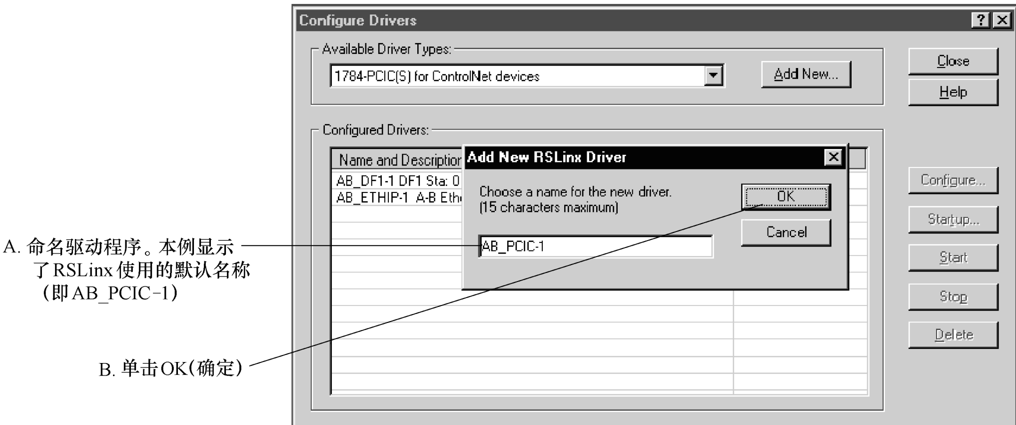
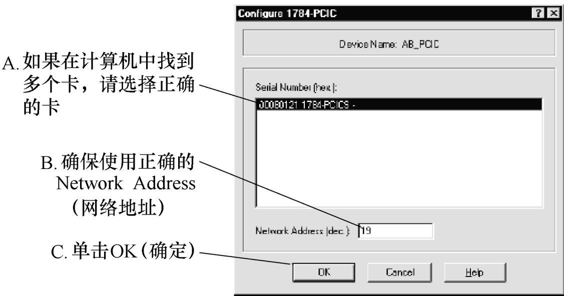


图4-85 命名ControlNet驱动程序

trolNet网络。远程I/O用ControlNet模块，加上开关量输入、输出模块，作为适配器连接ControlNet网络。要求实现的功能是，用运程开关量的输入去控制远程开关量输出。而各控制器对本地I/O的控制这里不讨论。



如果使用的卡类型不同，此屏幕的外观会有很大变化。

图4-86 与计算机内ControlNet模块相对应的配置

为了配置此系统，首先要通过RSLinx驱动程序将计算机连接到RSLogix 5000项目。其次是将ControlNet通信模块添加到RSLogix 5000项目中。最后是通过RSNetWorx预定ControlNet网络。以下分步骤分别进行介绍：

提示：在计算机上安装好RALinx软件，当开机后会自动运行此软件，以给RSLogix 5000编程软件或RSNetWorx网络配置软件提供联机路径选择。

1）创建工程。要使用RSLogix5000编程软件。具体步骤如下：

（a）选定控制器。运行RSLogix5000编程软件，点击File（文件）、New（新建），打开New Controller（新建控制器）画面。如图4-87所示填写控制器的型号（本例用1756-L1）、版本（本例为13）、名称（本例用ControlNet）、描述（可选，本例为Lab8），选择控制器类型、版本和所在槽位（本例选用4槽机架，控制器安装在0槽位），指定框架类型、工程保存目录（本例为D\

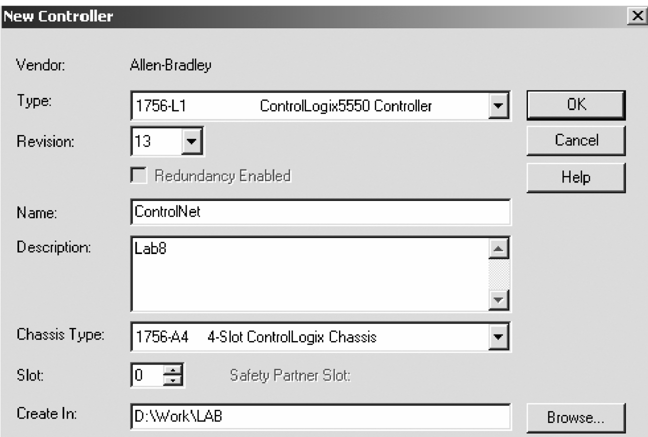


图4-87 选定控制器

Work \LAB）等相关信息，然后按 OK。

（b）添加本机架 CNB 通信模块。鼠标右键点击 I/O Configuration（I/O 组态，位于左边窗口的底部），并选择 New Module（新模块）。如图 4-88 所示，具体在模块列表中选择 1756-CNB/D。选中之后，按 OK。

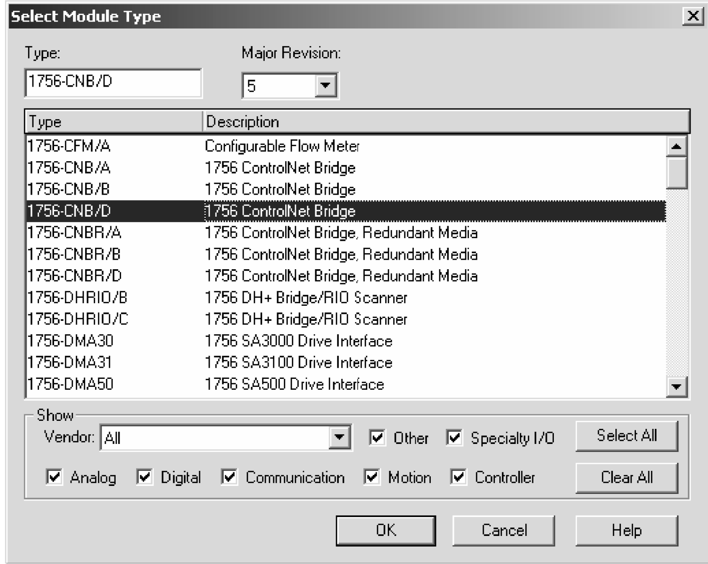


图 4-88 选择 New Module（新模块）

本例 CNB 通信模块位于 2 号槽，并且在 ControlNet 上的站点号（Node）上选 4 与硬件设置一致（硬件用模块上的拨码开关设置）。其他按图 4-89 所示填写模块相关信息，选定后点击 Finish。

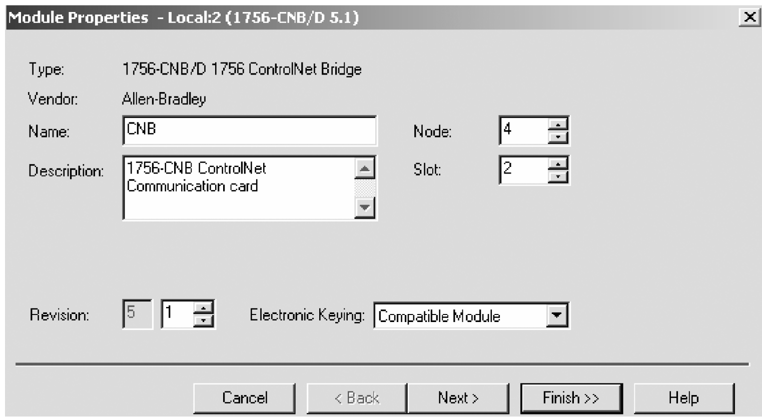


图 4-89 配置 ControlNet 模块

这里，Electronic Keying（电子锁）允许在 online（在线）之前确定一个物理模块与软件组态之间达到何种匹配程度。这种特性可以避免在不经意中将错误的模块插入错误的槽中。它有如下 3 种选择：

Compatible Module——物理模块的模块类型（Module Types）、目录号（Catalog Number）以及主要版本号（Major Revision）必须与软件组态匹配，次要版本号（Minor Revision）必

须大于等于软件指定的数值，否则 RSLogix 5000 将不接受所插模块。

Disable Keying——RSLogix 5000 不会检查模块版本的匹配情况。

Exact Match——物理模块的下列5个参数必须与软件组态匹配，否则 RSLogix 5000 将不接受所插模块：Vendor，Product Type，Catalog Number，Major Revision，Minor Revision（供应商、产品类型、目录号、主要版本号、次要版本号）。

（c）添加远程机架上的 CNB 模块。鼠标右键点击本机架 CNB 模块，选择 New Module。在模块列表中选择 1756-CNB/D。选中之后，按 OK。远程机架 CNB 通信模块位于运程机架的0号槽，并且在 ControlNet 上的站点号是5；机架类型为7槽。图4-90所示为填写模块组态信息。

图4-90　远程机架 ControlNet 模块组态

填好之后，按 Next，将出现如图4-91所示画面。可用其设置 RPI 时间，本例接受默认设置20ms。之后点击 Finish，又回到图4-91画面。并在其上也点击 Finish 即完成 ControlNet 模块配置。

图4-91　设置 RPI

（d）在远程机架上添加 IO 模块。办法是用鼠标右键单击远程 CNB 模块，选择 New Module。本例是，在模块列表中选择 1756-IB32/A（开关量输入模块），选中之后，按 OK。如图4-92所示填写模块组态信息。

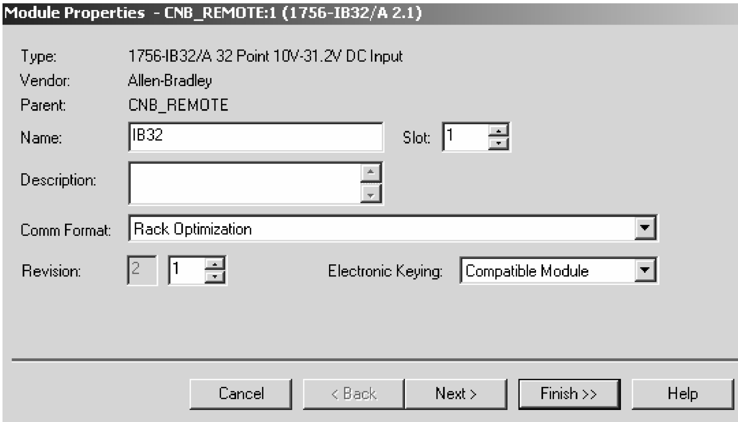


图 4-92　远程输入模块信息

其他的接受默认设置，选择 Finish。

再添加一个远程 DO 模块 OB16D（开关量输出），如图 4-93 所示填写模块组态信息，然后选择 Finish。

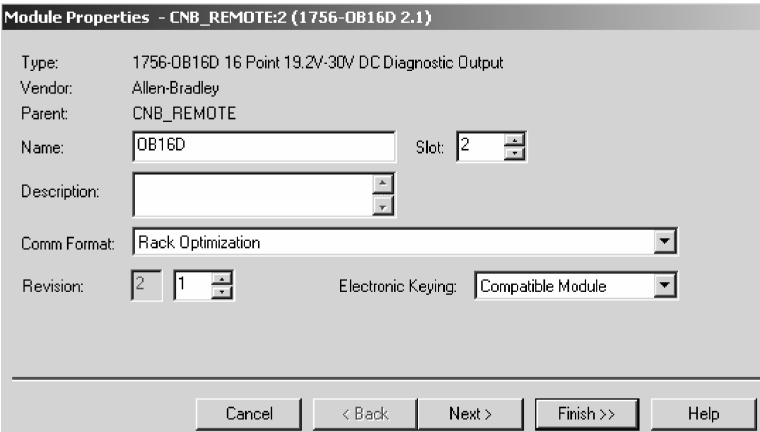


图 4-93　填写模块组态信息

（e）观察标签（Tag）。由于 I/O 标签在 I/O 模块配置后会自动生成，所以这时双击控制器标签，可观察到此标签。图 4-94 所示即为本例 I/O 标签。

P	Tag Name	Type	Base Tag	Alias For
	⊞-CNB_REMOTE:1:C	AB:1756_DI:C:0		
	⊟-CNB_REMOTE:1:I	AB:1756_CNB_SLOT:I:0	CNB_REMOTE:I.Slot[1]	CNB_REMOTE:I.Slot[1]
	⊞-CNB_REMOTE:1:I.Fault	DINT	CNB_REMOTE:I.Slot[1].Fault	
	⊞-CNB_REMOTE:1:I.Data	DINT	CNB_REMOTE:I.Slot[1].Data	
	⊞-CNB_REMOTE:2:C	AB:1756_DO:C:0		
	⊞-CNB_REMOTE:2:I	AB:1756_CNB_SLOT:I:0	CNB_REMOTE:I.Slot[2]	CNB_REMOTE:I.Slot[2]
	⊟-CNB_REMOTE:2:O	AB:1756_CNB_SLOT:O:0	CNB_REMOTE:O.Slot[2]	CNB_REMOTE:O.Slot[2]
	⊞-CNB_REMOTE:2:O.Data	DINT	CNB_REMOTE:O.Slot[2].Data	
	⊟-CNB_REMOTE:I	AB:1756_CNB_7SLOT:I:0		
	⊞-CNB_REMOTE:I.SlotStatusBits	DINT		
	⊞-CNB_REMOTE:I.Slot	AB:1756_CNB_SLOT:I:0[7]		
	⊟-CNB_REMOTE:O	AB:1756_CNB_7SLOT:O:0		
	⊞-CNB_REMOTE:O.Slot	AB:1756_CNB_SLOT:O:0[7]		

图 4-94　本例 I/O 标签

从图知，这里标签项很多。但对开关量输入、输出实际使用的只是 CNB_REMOTE：1. Slot ［1］ . Data. ＊ （＊为点号可选）及 CNB_REMOTE：1. Slot ［2］ . Data. ＊ （＊为点号可选）。其他的用故障处理或 I/O 设置。这也是 Logix5000 控制器与别的 PLC 又一区别之处。

（f）工程下载。回到 RSLogix5000 编程软件主画面，点击主菜单上的 Communication，选择 WhoActive，如图 4-95 所示，在路径中选中本地框架中的处理器模块，然后选择 Download。

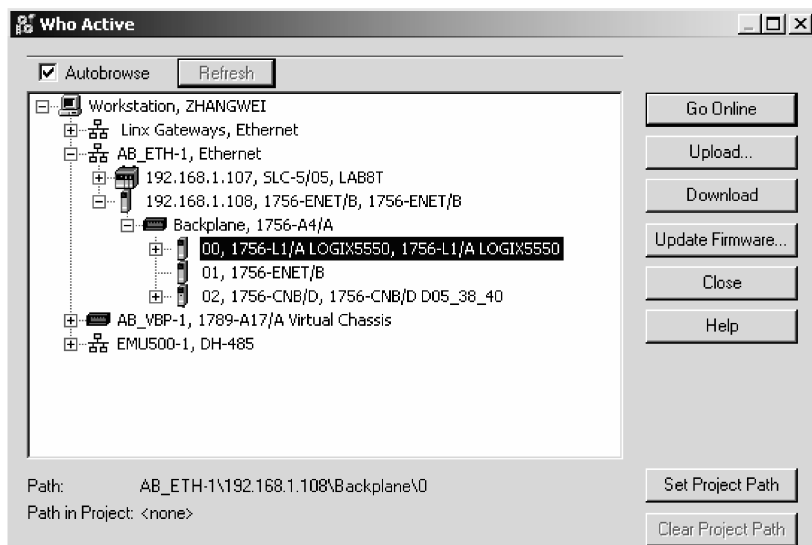


图 4-95　Who Active 画面

再利用菜单将控制器切换到 Rem Run（运程运行）模式，就可以验证本例工程了。但通过观察，发现 I/O not responding 的灯在处理器上闪动，并且远程 CNB 模块和远程 I/O 模块上有黄色的三角标记，如图 4-96 所示。这表明虽然已经用 ControlNet 连接了远程框架，但由于远程 I/O 数据属于预定（预定时段传输的数据）数据，需要进行控制网络规划（配置）后才能使用。否则就会出现上述不正常状态。为此，就要使用 RSNetWorx 软件，对 ControlNet 网络进行预定数据配置。

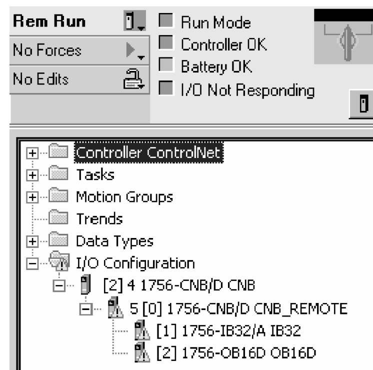


图 4-96　网络不正常显示

2）ControlNet 网络预定数据配置。要使用 RSNetWorx 软件。具体步骤如下：

（a）运行 RSNetWorx 软件，进入 ControlNet 组态界面。在工具栏上点击 Online 按钮，出现如图 4-97 所示网络浏览画面，再在其上选择网络路径。本例选中 ControlNet 网络。选中后点击 OK，以读取 ControlNet 网络上所有设备信息。

（b）读取网络上设备信息。接上所述，点击 OK 后，结合本例，所读取的网络上的设备信息如图 4-98 所示。读取完毕后，再选中 Edits Enabled 进入编辑模式。

（c）网络参数设置。这时，如图 4-99 所示，单击菜单 Network Properties（特性）项进行网络参数设定。

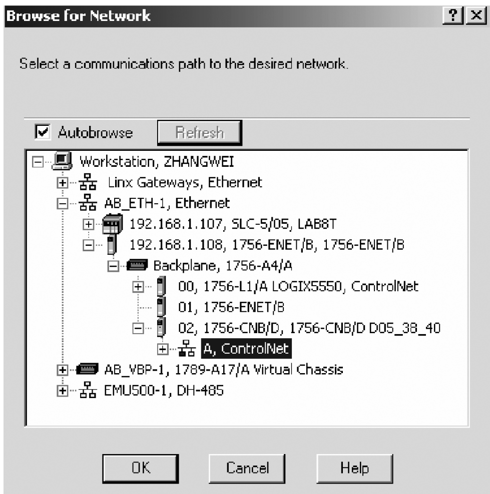


图 4-97　网络浏览画面

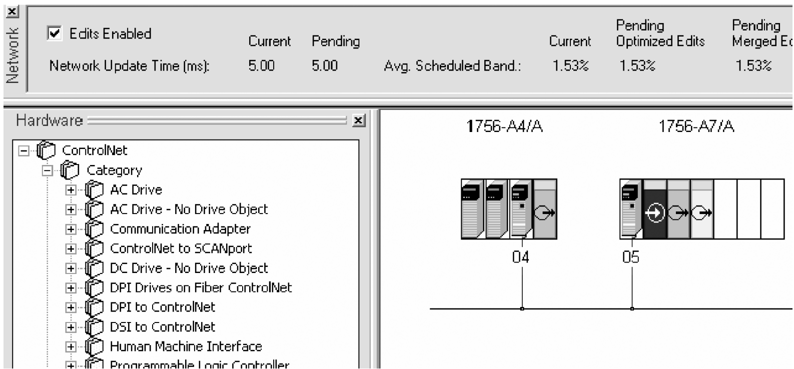


图 4-98　本例网络上设备

如图 4-100 所示，所示改变 Max Scheduled Address 为 5，改变 Max Unscheduled Address 为 10，然后点击 “OK”。

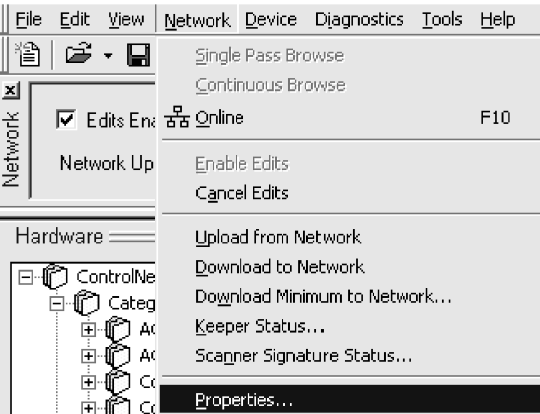


图 4-99　选定网络参数特性画面

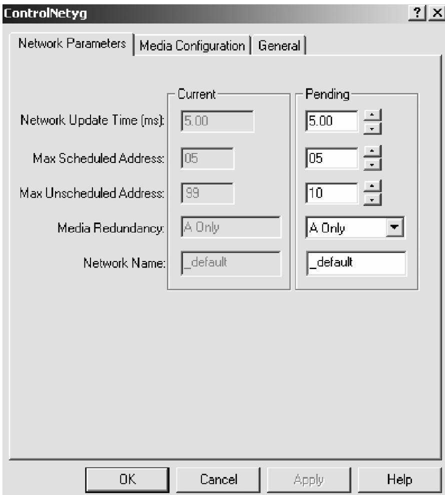


图 4-100　网络参数设定画面

3）保存设置。单击菜单栏的保存按钮，命名组态文件后选择 Save。在随后出现的画面中单击 OK 继续，网络组态信息被写入 CNB 模块。完成 ControlNet 网络的组态后，再回到 RSLogix5000 编程界面，在线观察，会发现如图 4-101 所示的网络正常情况。这时，远程机架 CNB 模块和 IO 模块上的黄色三角标记已经消失，并且处理器的 I/O 显示 OK。

完成以上步骤后余下的只是按控制要求编程了。编程时，远程 I/O 的使用与当地 I/O 实质上没有区别。所差的只是响应时间要考虑通信的延迟。具体编程略。

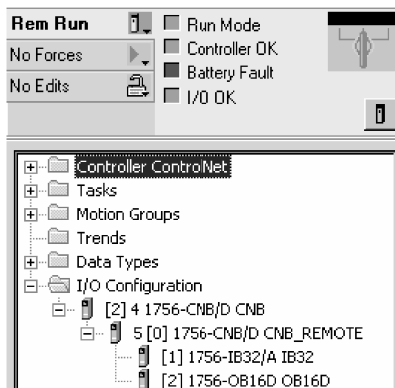


图 4-101　显示网络正常画面

（3）两或多个控制器连网配置

与上述用于远程 I/O 控制的配置不同的是远程机架上也配置有控制器，目的是通过 ControlNet 实现控制器间数据交换。各控制器所控制的本地与远程 I/O 这里不讨论。本例的配置过程大体与上述用于远程 I/O 控制的配置相同。只是在远程模块上要添加控制器，并要启动 RSLogix5000 编程软件又一例程，再建新工程，对其做相应设置。此外，为实现控制器之间标签链接通信，还要做数据生产者/消费者设置。具体设置于以太网中的标签链接类似，可参阅本书第 5 章第 3 节两个或多个控制器连网配置实例。

4.4.3　OMRON Controller Link

除了 DeviceNet 外，Controller Link 是 OMRON 公司目前主推的性能较高的控制网络。由于 OMRON 是 ODVA 组织的发起公司之一。所以，它的开放网络多可与 ODVA 的网络兼容。只是它的控制网不是 ControlNet，而是 Controller Link。

1. Controller Link 功能

（1）数据链接

这是 OMRON PLC 网络站点间传统的数据交换方式。只是 Controller Link 这个交换的数据量大，设置灵活（可人工设置，也可自动设置），所使用的链接区，如 I/O 区（CIO）、链接继电器（LR）、数据存储器（DM、EM）等，也可自由选定。同时，如果计算机配置有 Controller Link 网卡并运行有关软件也可参与这个链接，而且，它可链接交换的数据量更大。

（2）信息服务

PLC 运行网络指令（发送/接收及命令，SEND/RECV 与 CMND）实现站点间循时数据交换。而且，这个数据交换可跨网络进行。执行 SEND 指令可发送本 PLC 指定内存区的数据，自动写到目标站点 PLC 指定的内存区中。执行 RECV 指令可读取指定站点 PLC 指定内存区的数据，自动写到本 PLC 指定的内存区中。执行 CMND 可发送 OMRON FINS 协议的通信命令码，实现相应的通信操作。

（3）冗余功能

如使用光纤介质可实现介质冗余，使系统更加可靠。此外，安装 CS1W-CLK13、CS1W-CLK12-V1、CS1W-CLK53 或 CS1WCLK52-V1 两个模块到 CS1D（可冗余配置的 PLC），可组成 Controller Link 冗余网络。一个工作，另一个待机。一旦工作网络出现故障，待机的将自动接替其工作。这时，故障网络可以不必断电就可更换。

（4）特别提示

Controller Link 没有远程 I/O 功能，也没有远程主从通信功能。这就造成了它的控制站点都必须有中型以上 PLC CPU 模块。这样配置将增加网络配置成本，丧失了它原有系统配置成本低的优点。出现此情况的原因也许是因为，OMRON PLC 即使为大型机，但控制规模也不大。它的最高档 PLC CS1 机，其控制规模与 AB 的 ControlLogic 相比的，相差达一个数量级。后者的 ControlNet 网络，除用于 I/O 控制之外，还有很多远程 I/O 控制点数可增加，可从容地进行当地或其他连网控制，而 OMRON 的 CS1 机用于 I/O 控制之后，可能就没有多少远程 I/O 控制点数可利用了。

2. Controller Link 特点

（1）数据交换的延时是有限与可计算的

这与 Controller Link 是令牌网有关。如图 4-102 所示，在它的通信循环时间（Communications Cycle Time）中，有令牌循环周期（Token Circulation Cycle）及发牌周期（Polling Cycle）。其通信就是这通信循环不断重复的过程。

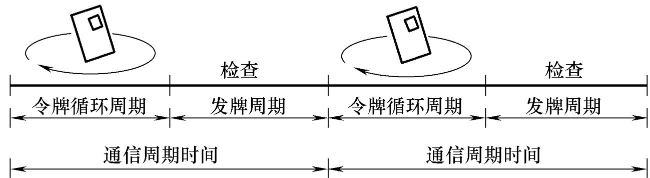


图 4-102　Controller Link 通信循环时间

在令牌循环周期，与其他令牌网络一样，取得令牌的站点如果有数据发送，可把数据与令牌一起发送。如果没有数据发送，则把令牌向下游传递。当令牌完成一周的传递，则又回到原始站点。这个过程周而复始，不断重复。

在发牌周期，一个称呼叫（Polling Node）的站点，正常情况为站址最低的站点，管理令牌、检测网络及传递网络参数设置。而其他站点，称为被呼叫（Polled Nodes）站点，接受检测及网络设置。

Controller Link 通信循环参数主要有：最大站址，每通信循环周期被呼叫站点数及每通信循环事件帧数。这帧数以 128 个字节为单位，最多可设为 35 个，4480 字节。事件帧主要用于信息服务。所有这些参数可通过 OMRON 提供的网络配置软件处理。

做了网络配置，再针对不同型号的 PLC 及可计算出数据交换延时，OMRON 的 Controller Link 用户手册就有计算实例。可知，Controller Link 网络的数据交换的确定性是得到保证的。

（2）通信介质可以选用双绞线，也可选用光纤

双绞线介质 价格便宜，并便于安装与维护。光纤介质有超强抗干扰能力，允许组建长距离、大范围的网络。使用 H-PCF 光缆通信距离总长可达 20km（最大站点间距 1 km）。使用 GI 光缆通信距离总长可达 30km（最大站点间距 2 km）。如果使用特殊光缆连接器，光缆也很容易连接或断开。

（3）灵活的网络间互连

Controller Link 可通过 CS、CJ 系列 PLC，与其他 OMRON 网络，如以太网、SYSMAC NET、SYSMAC LINK 和另一个 Controller Link 互连。办法是，这些 PLC 除了安装 Controller

Link 模块，还要安装其他网络模块。这样互连后，信息服务就可在跨（可跨三层）网络实现。与 ControlNet 不同的是，它必须在安装多种（个）通信模块的站点（网桥）做网络路由表设置，标明相互连接的网络地址。而 ControlNet 无须设置路由表，用 RSLinx 软件即可处理路由。

（4）有多种中继器

可用以连接 T 分支器，或延长网络距离，或扩展网络规模，或转换网络介质，为网络安装及使用提供更大的方便。

（5）可进行网络状态实时监控

如出现错误，将记录出错代码及出错时间。这些状态数据将存放在 Controller Link 模块的状态存储区中。最多可存储 39 个记录。

3. Controller Link 拓扑结构

（1）双绞线电缆拓扑结构见图 4-103。

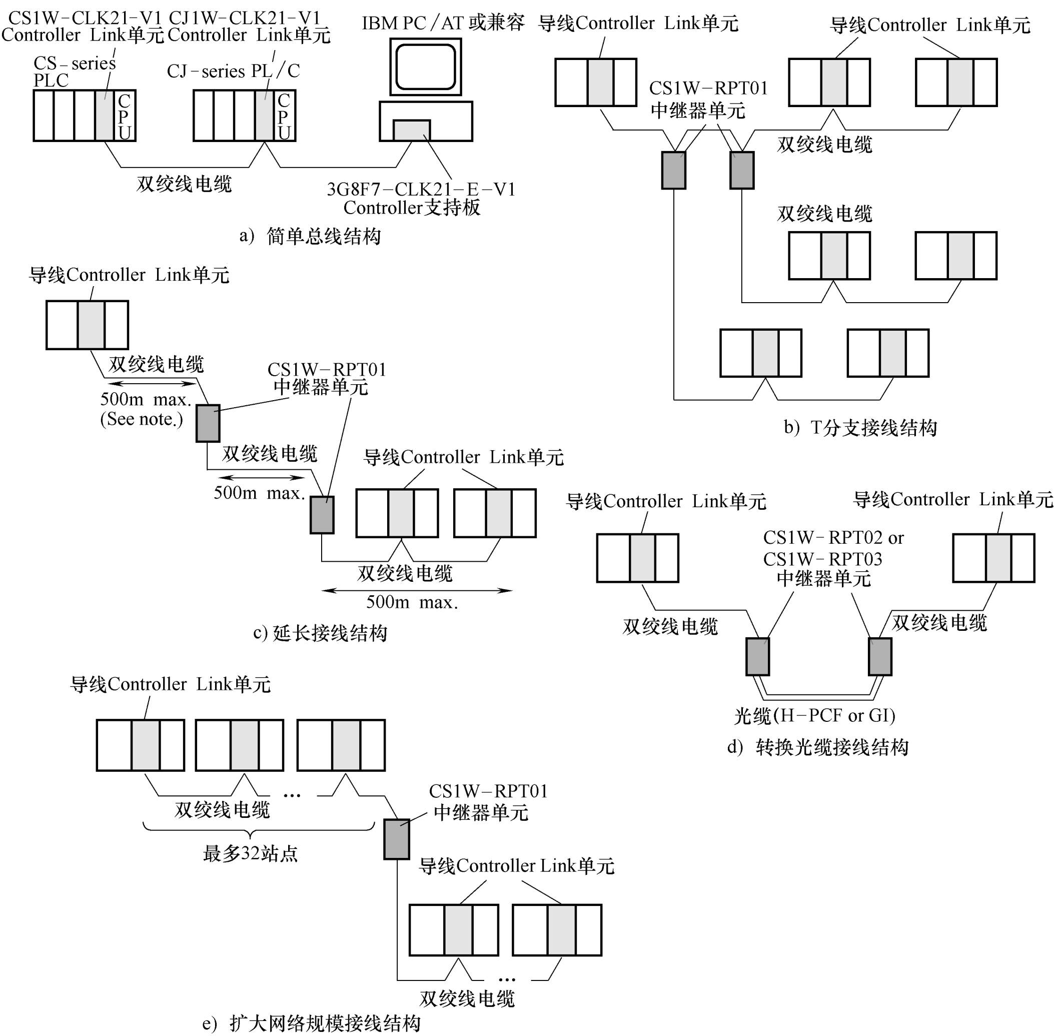


图 4-103　电缆拓扑结构

（2）光缆拓扑结构

不论哪种光缆，其结构都为如图 4-104 所示。

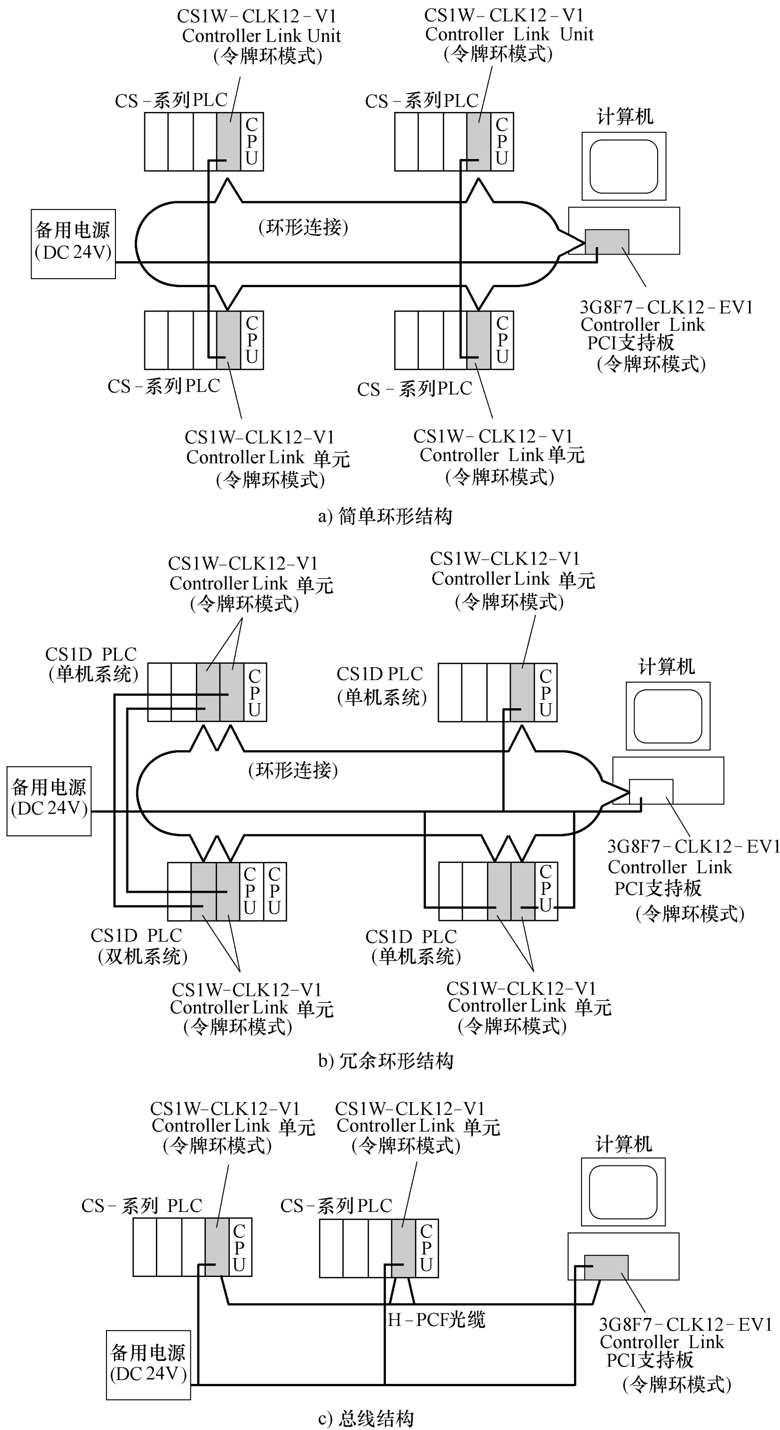


图 4-104　光缆拓扑结构

4. Controller Link 性能规格

表 4-27 所示为它的版本 CLK21 模块性能规格。

表 4-27　Controller Link 版本 CLK21 性能规格

项　　目	规　　格
通信方式	N:N 令牌总线
编码	曼彻斯特编码(Manchester Code)
调制解调	基带编码(Base Bonud Code)
同步方式	标志同步(符合 HDLC 帧)
传输通道方式	多站总线式
波特率和最大传输距离	最大传输距离随波特率而变,如下所示: 2Mbit/s:500m 1Mbit/s:800m 500Kbit/s:1km
媒介	指定的屏蔽双绞线电缆,信号线数:2,屏蔽线数:1
节点连接方式	PC:连接至端子板 IBM PC/AT 或兼容机:通过专用插件连接(附件)
最大节点数	32 个节点
通信功能	数据链接和信息服务
数据链接字数	每个节点的传送区域:最多 1000 字(2000 字节) 一台 PC 中的数据链接区(C200HZ/HX/HG/HE 或 CV 系列 PC)(发送/接收):最多 8000 字(16000 字节) 一台 IBM PC/AT 或兼容机中的数据链接区(发送/接收):最多 32000 字(64000 字节) 一个网络中数据连接的字数(传送总数):最多 32000 字(64000 字节)
数据链接区域	位(bit)区(IR,AR,LR,CIO),数据存储器(DM),和扩展数据存储器(EM)
信息长度	最多 2012 字节(包括字头)
RAS 功能	发牌节点后备功能 自诊断功能(启动时的硬件检查) 回送测试和广播测试(使用 FINS 命令) 监视定时器 出错记录功能
错误控制	曼彻斯特编码(Manchester Code)检查 CRC 检查(CCITT $X^{16}+X^{12}+X^5+1$)

5. OMRON Controller Link 组件

主要组件是通信模块。再就是中继器及附件。通信介质是标准产，有的 OMRON 也提供。

(1) Controller Link 通信模块

中、大型机，如 CS1、CJ1 新型机及 C200Ha、CVM、CQ 等老机型，才有此模块。不同 PLC 型号有不同的模块。其功能相同，但性能略有差别。多数模块可使用的介质为双绞线。大型机用的还有可使用光纤介质的模块。CSD1 机还可冗余配置。图 4-105 所示为 CJ1 机使用双绞线介质的 CLK21-V1 模块外观。

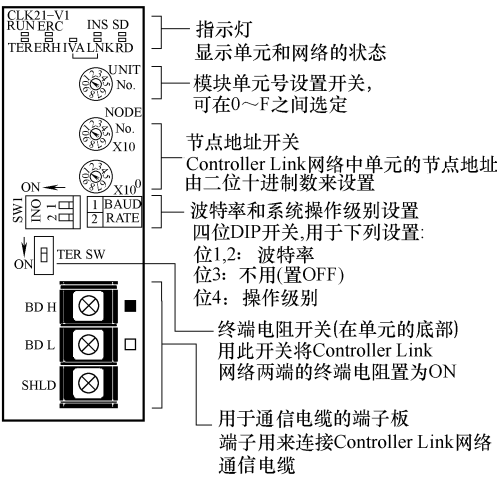


图 4-105　CLK21-V1 模块外观

从图知：它有指示灯，可显示网络及模块状态。有单元号设定开关，用以设定单元号以作为这个通信模块在 PLC 中的标识，进而 PLC 为其分配与这个单元号相对应的工作区（CIO 及 DM 区）。站址设置开关，用以设置该模块在网络中的地址以作为站点在网络中的标识。波特率设置开关，用以设置波特率。终端电阻开关，如果模块处网络终点，用此开关可连接终端电阻。连接电缆的接线端子，用以连接双绞线。

（2）计算机 Controller Link 支持插板

有 3G8F7-CLK21-E 及 3G8F7-CLK11-E 两种。前者用于连接双绞线介质，后者用于连接光纤介质。计算机插入这个插板，并安装 OMRON 提供的 Controller Link 支持软件，也可计算机接入 Controller Link 网，并成为它的一个站点。而且，如用它做数据链接，将比 PLC 有更大的数据交换量。只是这样插板、软件价格高，用于监控也不太方便。实际应用不多。

提示：即使没有这里提到的插板，计算机运用 OMRON 编程软件或网络配置软件，做好设置，利用标准串口或 USB 口与网络所在的一个 PLC 联机，也可配置、监视 Controller Link 网络。

（3）Controller Link 中继器

有线到线中继器，还有线到光缆中继器。其外观如图 4-106 所示。

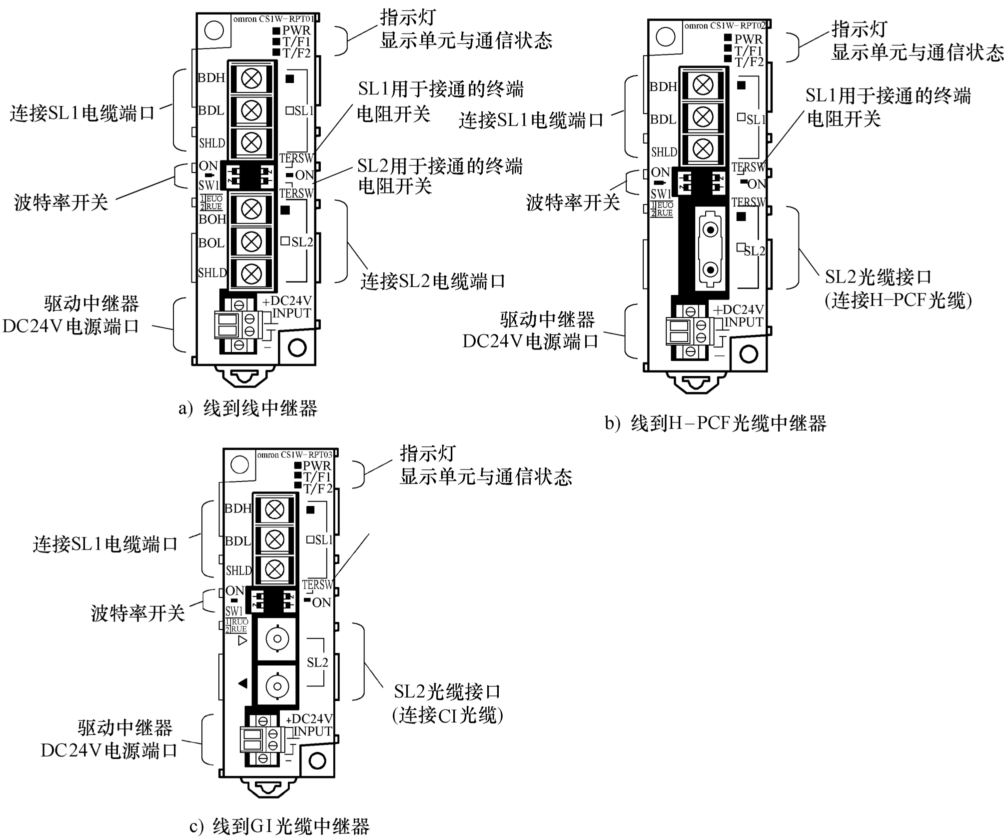


图 4-106 不同中继器

从图知：它有指示灯，可显示网络及模块状态。终端电阻开关，如果需要可连接终端电阻。连接电缆或光缆的端口，用以连接双绞线或光缆。波特率设置开关，用以设置波特率。

电源接口，用以为中继器连接 24V 直流电源。

（4）其他组件

除了通信介质、连接器之外，还有编程软件及网络配置软件。这些都集成在 OMRON 提供的 CX-ONE 软件中。计算机插板用软件则另做采购。

6. Controller Link 网络数据链接设置

Controller Link 网络主要用于 PLC 间的链接通信。所以它的设置也是网络的最基本设置。以下对它的链接模式及其设置方法做简要介绍。至于怎么更具体的设置将在随后介绍实例中说明。

（1）设置模式

有自动对等分布模式、自动 1∶*N* 模式及人工模式。

1）自动对等分布模式。可用于设置简单的链接。图 4-107 所示为一例简单链接。它有 4 个站点。各有位数据区及字数据区。站点 1 写（发送）发送区为数据区#1，而站点 2、3、4 的数据区#1 则为它的读（接收站点 1 的写区数据）区。通信完成后，站点 2、3、4 数据区#1 的内容，与站点 1 的数据区#1 的内容一致。与此类似，数据区#2，为站点 2 的写区，数据区#3 为站点 3 的写区。

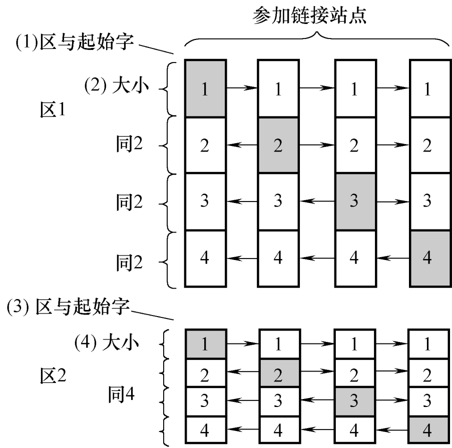


图 4-107　所示为一例简单链接

上图组 1 可以是位链接，用 CIO 或 LR（OMRON PLC 的继电器），组 2 是字链接，用 DM（OMRON PLC 的数据存储区）。在每区#1、#2、#3及#4 的发送部分的大小事相同的，并按站址升幂确定。所有站点都可设置为参与链接或不参与链接。设置为参与链接的不能只接收部分数据，而必须接收全部别的站点发送的数据。

这简单链接设置可使用编程工具，如简易编程器，对站点与单元号对应的 DM 区（参数设置区）按要求赋值。也可用编程软件设置。

2）自动 1∶*N* 模式。之下还分有 3 种模式：公用型（Common Type）、1∶1 型（1 to 1 Type）及链接型（Chain Type）。图 4-108 所示为这样设置的实例。

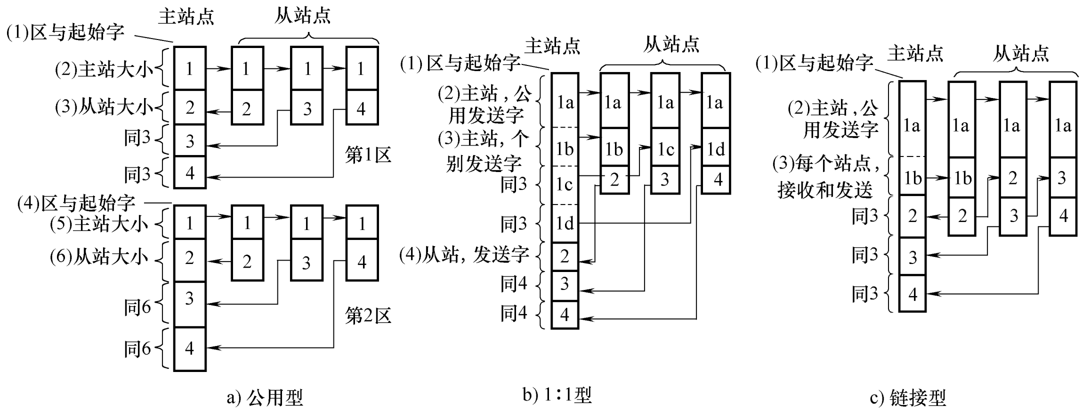


图 4-108　自动 1∶*N* 模式设置

上述图 4-109a 为公用型。只能在主从站之间交换数据，从站之间不直接交换数据。图 4-109b 为 1 对 1 型。主站除了向从站发送公用数据，还可 1 对 1 向从站发送数据。图4-109c 为链接型。除了主站向从站发送公用数据，还有一组各站点间依次链接地发送与接收数据。

除了以上大小是相同的分配，上述再就是自动设置也可做偏移设置。

要指出的是 OMRON 接入 ControllerLink 网络的 PLC 性能（主要是数据内存区大小，即内部器件）差别很大。所以，同等性能的在一起链接还好处理，而高低性能 PLC 在一起链接就要受到不少限制。具体链接细节还得参阅有关型号 PLC 的说明书。

3）人工设置。人工设置较灵活，可满足特殊需要。具体是指定 PLC 的数据区（如 DMEM 等）作为链接区。图 4-109 所示为两个站点间两组可能的数据链接。

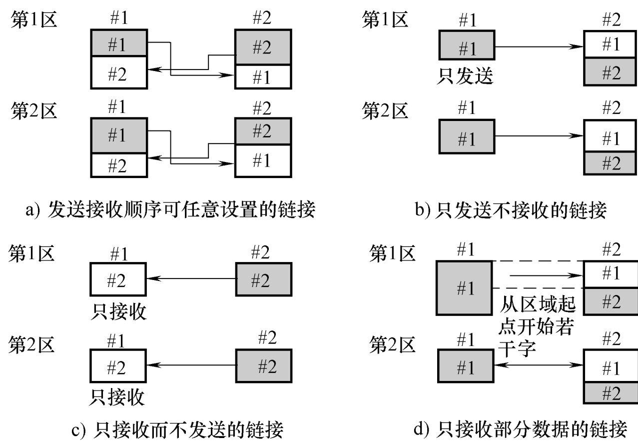


图 4-109　多种可能的链接

此外，还可偏移链接。这时可指定接收链接数据区的起始位置及接收链接数据区的大小。如图 4-110 所示，这里站点 2 指定只接收站点 1 发送的偏移部分的数据。这样链接的好处是，接收站点无需的数据不予接收，可充分利用 PLC 的资源。

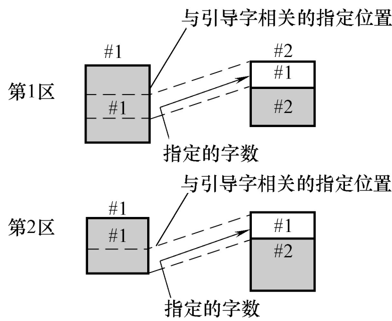


图 4-110　偏移链接

（2）设置方法

可使用简易编程器，也用计算机。

1）使用简易编程器。为此，对通信模块所使用的 PLC 内存区（CIO、AR、DM 等内部器件）要有所了解。然后根据使用要求对这些器件赋值。图 4-111 所示为 CS1 机的 DM N 的含义。这里 N 按下式计算：

$$N = \mathrm{DM30000} + 100 * \text{单元号}$$

从图可看出，这里各个位的取值都有一定意义。其他的与模块工作相关的类似内部器件的含义，OMRON 产品说明书都有详细说明。为了实现网络上的 PLC 能数据链接，自然要逐一对联网的 PLC 都要做类似上述的模块设置。用简易编程器设置简单，但要记住很多内存区的含义，不易实施。较好的办法是用计算机。

2）使用计算机。要运行编程软件及网络软件。

（a）编程软件为 OMRON 的 CX-Programmer。运行它建立新工程后，在 I/O 表上，添加

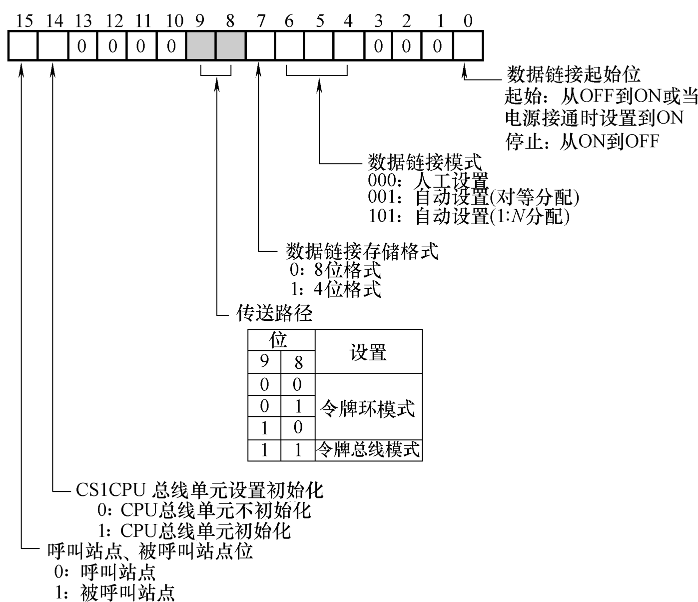


图 4-111 CS1 机的 DM *N* 含义

该模块。如图 4-112 所示，在空槽 0000 上添加单元号位 0 的 CJ1W-CLK23 模块。

再添加后的 PLC IO 表上，双击该模块项，将弹出如图 4-113 所示的察看参数窗口。

如图已显示的参数组为“All parameters”（全部参数）。如其中“Pollingnode/polled node bit”（呼叫/被呼叫）项，该例选定呼叫。其他也类似，可按要求对其逐项选填。选填后，点击《确定》即完成模块设定。当然要联机（可使用串口）下载给 PLC 才能生效。

为了实现网络上的 PLC 能数据链接，自然也要逐一对联网的 PLC 都要做类似上述的模块设置。

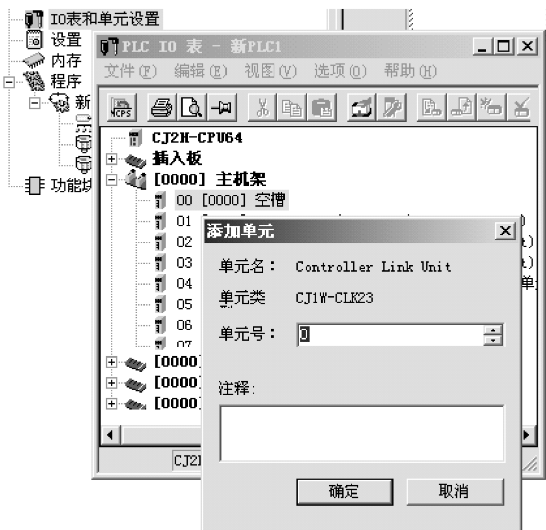


图 4-112 添加 CJ1W-CLK23 模块

（b）网络软件有单独使用的 ControllerLink 网卡支持软件及集成在 OMRON CPX-one 中的网络管理软件 CX-Integrator。如何使用见随后的应用实例。

7. ControllerLink 系统配置实例 1

本例有 4 个 CJ PLC 站点，对其做简单链接。其网络及其链接配置分述如下：

（1）用编程 CX-programmer 软件做模块配置

要分别对 4 个 CJ 机做好 I/O 配置。并分别如上所述，打开各个 Controller Link 模块的“察看参数”页，按设计要求，对其中参数逐一选定。所有站点都设置为参与链接，数据链



图 4-113　察看参数窗口

接模式，都设置为手工链接。站点 1 PLC 设置为呼叫（Polling）站点，其他都为被呼叫（polled）站点。等等。

（2）用 CX-integrator 软件做网络配置

其过程先是在新工程中创建网络 1，然后在网络中添加网络部件。

1）创建网络 1。如图 4-114a 所示，打开软件后，点击主菜单“插入”下的“网络”项。将弹出如图 4-114b 所示的“向导-网络/组件设置”窗口。

之后，如图选择 ControllerLink，并点击“下一步”。将弹出如图 4-115 所示的“向导-网络设置”窗口。

在该窗口上，输入网络名为“网络 1”，网络地址为“1”，然后点击“完成”。将完成网络建立，有回到软件的主窗口。但如图4-116 所显示，这时已建立了网络 1。



a) CX-integrator 软件



b) 向导-网络/组件设置窗口

图 4-114　CX-integrator 软件及向导-网络/组件设置窗口



图 4-115　向导-网络设置窗口

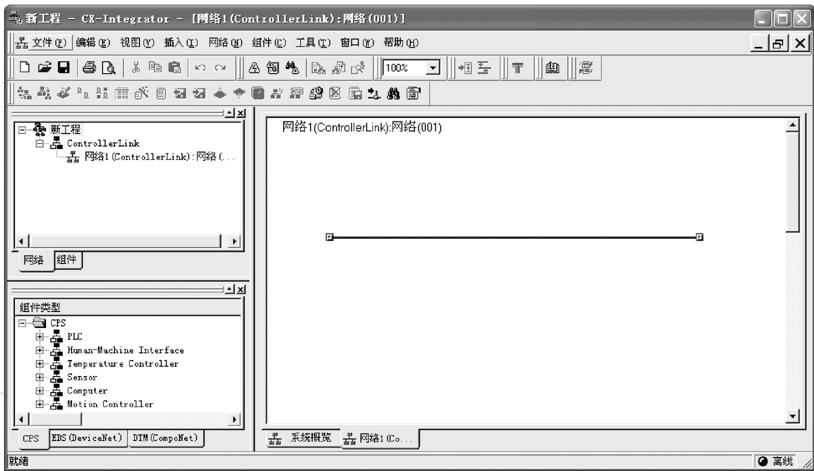


图 4-116　显示已建立网络 1 主窗口

2）插入组件。在图 4-117 点击“插入”项下的“组件”菜单项，将弹出如图 4-117 所示“向导-网络/组件配置”窗口。

在该窗口选择“PLC”，并点击“下一步”，将后弹出的可选择组件的“向导-组件设置”窗口（此窗口显示这里略）。本例选择 PLC 机型为“CS1G-CPU44H”。再点击其上的“下一步”，将转换如图 4-118 所示的可输入组件名称的“向导-组件设置”窗口。本例用第一站的组件缺省名为“Compo1”，其余依次为“Compo2”、“Compo3”、“Compo4”。



图 4-117　向导-网络/组件配置窗口



图 4-118　可输入组件名称的“向导-组件设置”窗口

在该窗口上，点击下一步，将弹出“向导-组件设置-单元类型”窗口。如图 4-119 所示，本例选单元类型为“CS1W-CLK21-V1”。



图 4-119　单元类型 CS1W-CLK21-V1 选定窗口

在该窗口上，点击“下一步”，将弹出“向导-组件设置-单元号”窗口。如图 4-120 所示，本例选单元号“00”。要注意的是，此单元号要与拨码开关选定一致。

在该窗口上，点击“下一步”，将弹出“向导-组件设置-节点地址”窗口。如图 4-121 所示，本例组件地址为“节点 1”。要注意的，



图 4-120　所示，单元号“00”选定窗口

4 个站点的此地址应不同，并与拨码开关一致。之后点击“完成”。

再依次插入节点号为 2 、3 及 4 的站点。都完成后，即完成了网络设置。并在软件主窗口上将出现如图 4-122 所示的画面。



图 4-121　所示，选节组件地址窗口

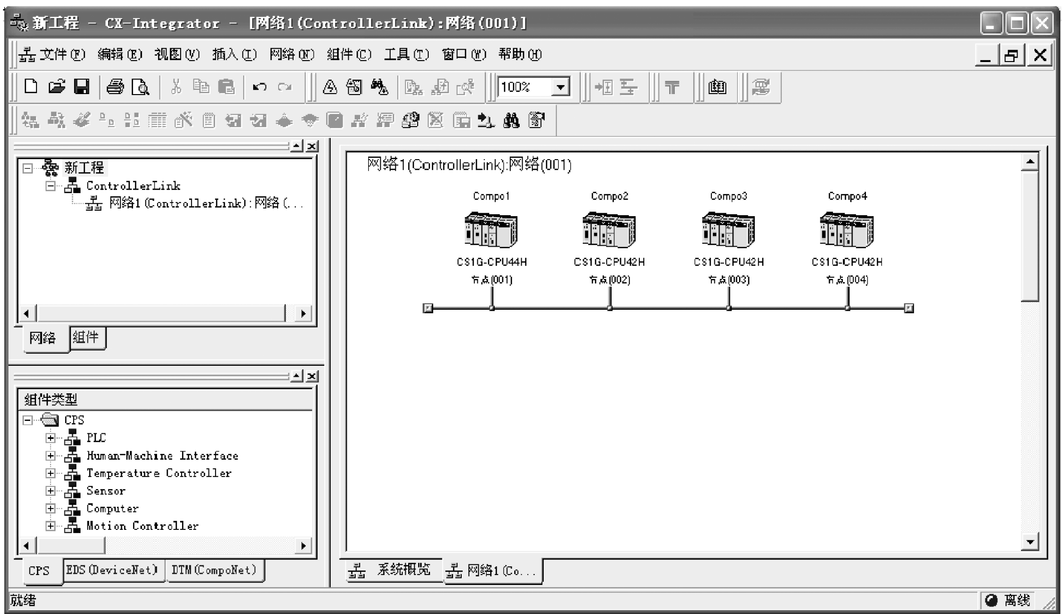


图 4-122　插入 4 个站点后主窗口画面

提示：在图 4-122 所示窗口上，双击各站点的图标也可弹出如图 4-122 所示的“察看参数”窗口，仍可看到或修改当时的编辑结果。

（3）用 CX-integrator 软件做链接配置

其过程先是点击如图 4-122 所示窗口的“工具”菜单项下的“启动数据链接”项，将弹出如图 4-123 所示的“选择网络”窗口。本例选择“Controller link”。

点击其上的“确定”后，将弹出如图 4-124 所示的空白的“数据链接组件”窗口。在其上可一个个选择参与链接的组件，并对数据链接再一步步设置。

点击该空白窗口上的“表”菜单项下的“向导”项，将弹出如图 4-125 所示的“数据链接向导”窗口。本例为 4 个站点链接，故在“网络节点处”键入 1，2，3，4。

再点击该窗口“下一步”，将弹出如图 4-126 所示节点 1 的“数据链接向导”窗口。本例用默认值，节点 1 的内存用 CIO 及 D 区，起始地址为 0。尺寸为 10（字）。



图 4-123　选择 Controller Link 网络窗口

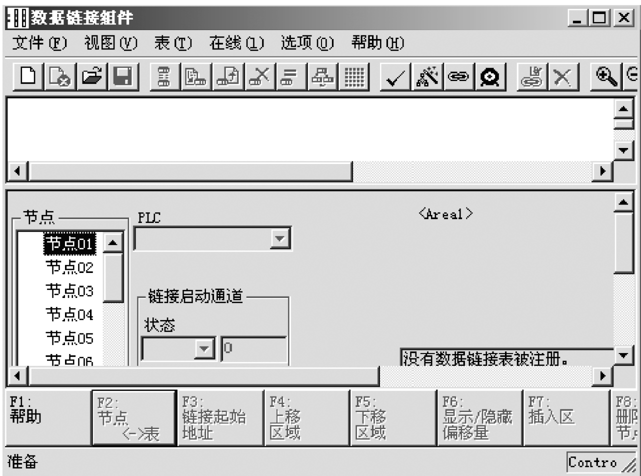


图 4-124　空白“数据链接组件”窗口

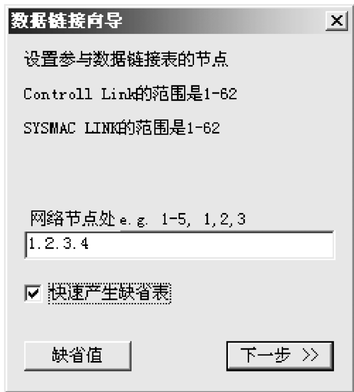


图 4-125　数据链接向导窗口

在该窗口，再点击“下一步”，将对节点 2 做设置。一直继续下去。直到设置完节点 4，再点击“下一步”，将弹出如图 4-127 所示已完成数据链接设置“数据链接组件”窗口。

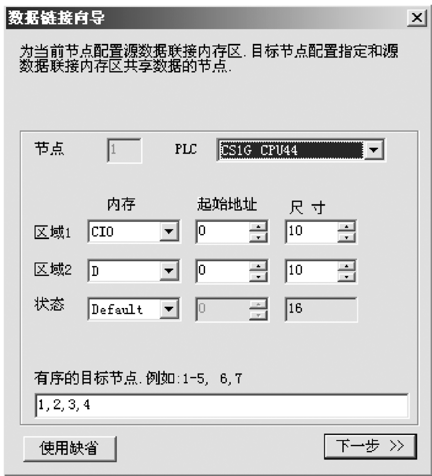


图 4-126　节点 1“数据链接向导”窗口

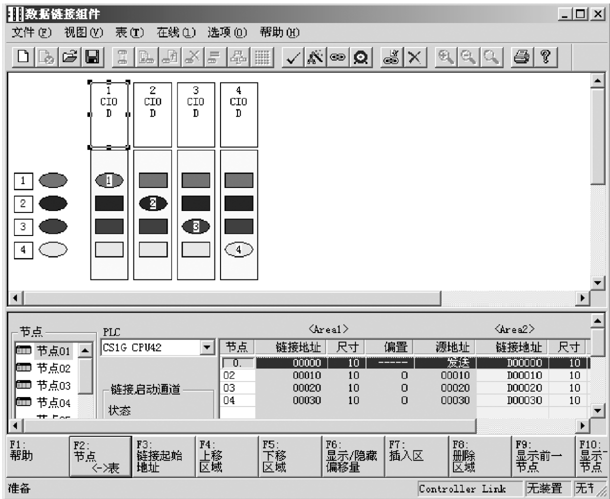


图 4-127　完成设置“数据链接组件”窗口

该窗口的上部用图形显示各节点的发送区（用椭圆图形）与接收区（用长方形），较为形象。窗口的下半部用表格显示各节点链接的链接地址、尺寸、源（发送）。图中显示的为节点 1 的情况。点击该图左下方的不同的节点号可显示不同节点的链接情况。

完成链接后，还可点击“表”菜单项下的“证实表的有效性”项，还可检查所作的设置是否正确。如出错将有提示。

所有设置完成后还要联机，把上述设置下载给各个 PLC。PLC 再重新上电使设置有效，PLC 进入运行模式，并起动链接即可实现链接通信。

8. Controller Link 系统配置实例 2

本例也是 4 个站点，与实例 1 不同的它用 1∶*N* 配置。在链接设置时用自动主从模式。其具体过程为

（1）用编程 CX-programmer 软件做模块配置

要分别对 4 个 CJ 机做好 I/O 配置。并分别如上所述，打开各个 Controller Link 模块的“察看参数”页，按设计要求，对其中参数逐一选定。也是所有站点都设置为参与链接，但数据链接模式，都设置为自动 1∶*N* 模式。站点 1 PLC 也设置为呼叫（Polling）站点，其他也都为被呼叫（polled）站点。等等。

（2）用 CX-integrator 软件做网络配置

先是全部联网 PLC 接好线，全部在线工作。然后运行 CX-integrator 软件，创建新工程，建立网络 1。并与呼叫站点联机。在出现的“数据链接组件”窗口上，点击其上“在线”主菜单下的“自动设置链接”项，进而将弹出如图 4-128 所示的“Automatic Datalink”窗口。

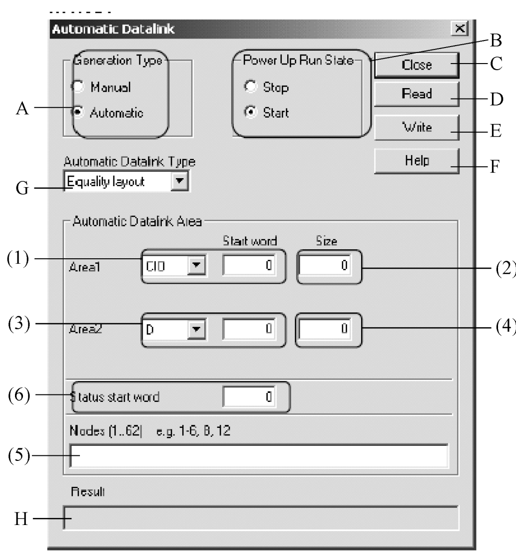


图 4-128　Automatic Datalink 窗口

从图知，自动链接模式为对等模式。图中各项限定含义见表 4-28 所示。

表 4-28　自动对等模式各项选定含义

No	项目	功能描述	No	项目	功能描述
A	一般	选择自动	G	自动数据链接	按如下选择数据自动链接： 对等分配 通用(1∶*N* 设置) 1 比 1(1∶*N* 设置) 链接(1∶*N* 设置)
B	加电并运行	选择当 PLC 加电后自动数据链接起始			
C	关闭	关闭自动数据链接			
D	读	自 PLC 读设置			
E	写	写设置到 PLC			
F	帮助	显示帮助	H	效果	当点击读、写按钮时，显示状态

也可选定自动链接公用（Common）型。也可选用 1 对 1 型，或及链接型。则出现的窗口分别如图 4-129 ~ 图 4-131 所示。其各项选定含义则分别见表 4-29 ~ 表 4-31 所示。

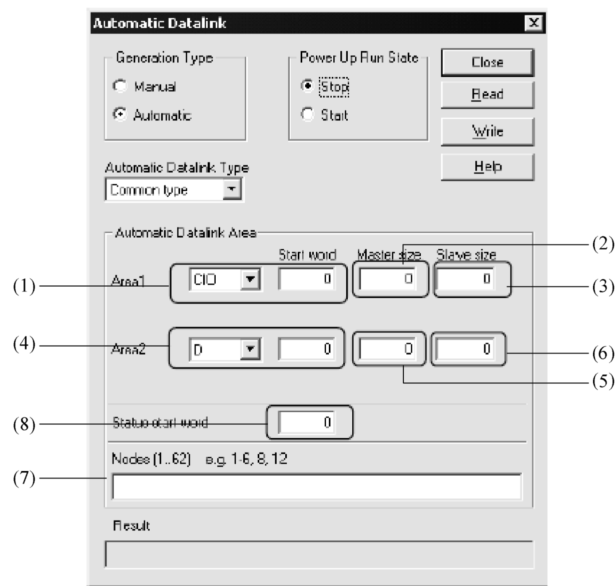


图 4-129　Automatic Datalink 窗口（公用型）

表 4-29　自动 1:*N* 模式公用型各项选定含义

No	项目	功能描述	No	项目	功能描述
A	一般	选择自动	G	自动数据链接	按如下选择数据自动链接： 对等分配 通用(1:*N* 设置) 1 比 1(1:*N* 设置) 链接(1:*N* 设置)
B	加电并运行	选择当 PLC 加电后自动数据链接起始			
C	关闭	关闭自动数据链接			
D	读	自 PLC 读设置			
E	写	写设置到 PLC			
F	帮助	显示帮助	H	效果	当点击读、写按钮时，显示状态

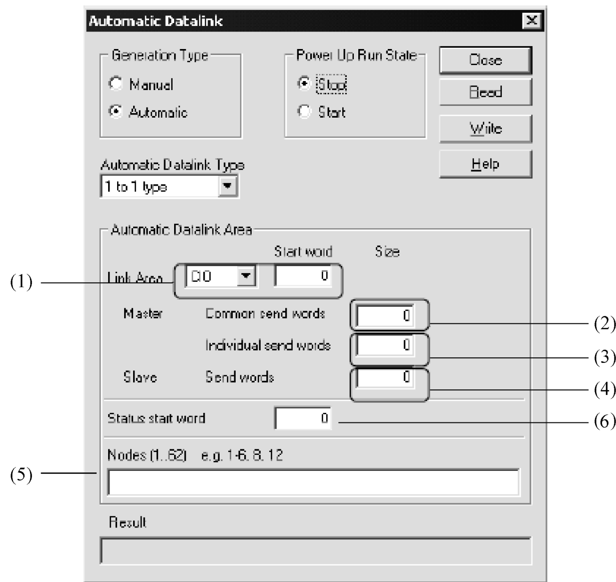


图 4-130　Automatic Datalink 窗口（1 对 1 型）

表 4-30　自动 1:N 模式 1 对 1 型各项选定含义

No.	项　目	功 能 描 述
(1)	链接区与起始字	设置链接区与起始字
(2)	主站,共同发送字	设置自主站向全部从站发送数据量。到个站点数据量相等
(3)	主站,个别发送字	设置自主站向各个从站发送数据量
(4)	从站,发送字	设置各个从站向主站发送数据量
(5)	站点	设置参与链接的站点
(6)	状态起始字	设置存储数据链状态的起始字(如设置 0,则使用全部缺省区)

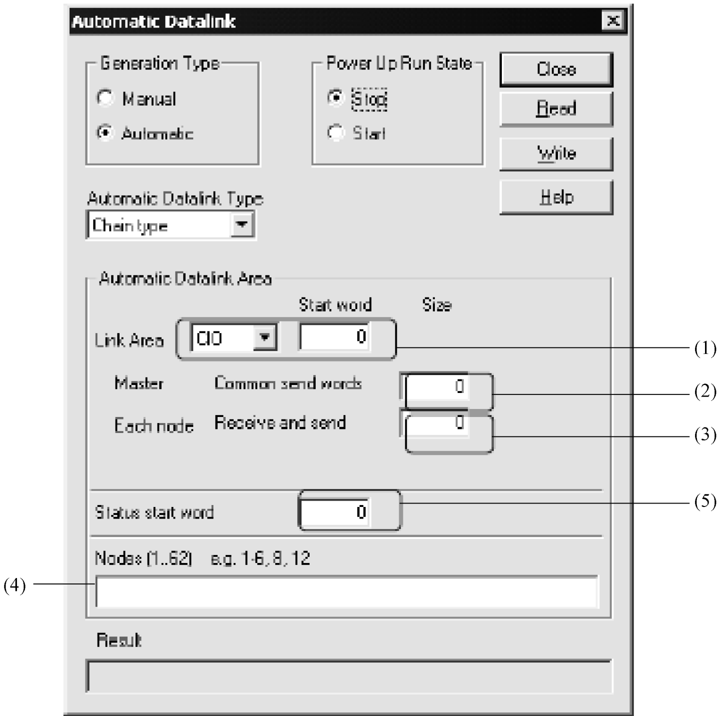


图 4-131　Automatic Datalink 窗口（链接型）

表 4-31　自动 1:N 模式链接型各项选定含义

No.	项　目	功 能 描 述
(1)	链接区与起始字	设置链接区与起始字
(2)	主站,共同发送字	设置自主站向全部从站发送数据量。到个站点数据量相等
(3)	各站点接收与发送	设置各站点发送到下一站点数据量
(4)	站点	设置参与链接的站点
(5)	状态起始字	设置存储数据链状态的起始字(如设置 0,则使用全部缺省区)

做好选定、下载给 Polling PLC，各站点有都做好了相应设置，PLC 重新上电连网，即可按上述设置工作。自动设置比手工要简单些。但要联机在线进行，稍有不便。

4.5　Profibus

关键词：1 级（类）主站、2 级（类）主站、DP 从站、DP 通信、DX 通信、单主多主、令牌、DP-V0、DP-V1、DP-V2、GSD

4.5.1 Profibus 简介

Profibus 由 3 个兼容部分组成，即 Profibus-DP（ Decentralized Periphery）、Profibus-PA（Process Automation）及 Profibus-FMS（Fieldbus Message Specification。Profibus-DP）用于控制器与分散式 I/O 或作为从站的其他控制器之间通信。Porfibus-PA：专为过程自动化设计，可使传感器和执行机构联在一根总线上，并有本征安全规范。Profibus-FMS 用于控制器之间相互通信，是 DP 的先驱。此外，还有运功及安全控制用 Profibus，而 PLC 主要用的是 Profibus-DP。

1. Profibus-DP 组成

Profibus-DP 为多主多从结构，可方便地构成集中式、集散式和分布式控制系统。可能有以下 3 种系统配置：纯主-从系统、多主站系统及纯主-主系统。在同一总线上最多可连接 126 个站点。

（1）纯主-从系统

在总线系统的运行阶段，只有一个活动主站，如图 4-132 所示，PLC 作为主站。

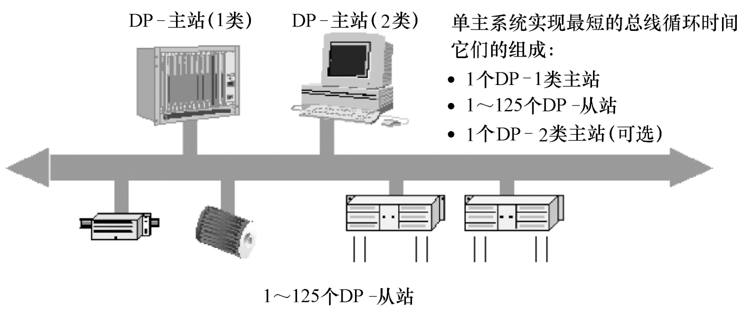


图 4-132 单主站系统

（2）多主站系统

总线上连有多个主站。这些主站与各自从站构成相互独立的子系统。每个子系统包括一个 DPM1、指定的若干从站及可能的 DPM2 设备。任何一个主站均可读取 DP 从站的输入/输出数据，但只有一个 DP 主站允许对 DP 从站写入数据。如图 4-133 示，它有 3 个主站，多个从站。

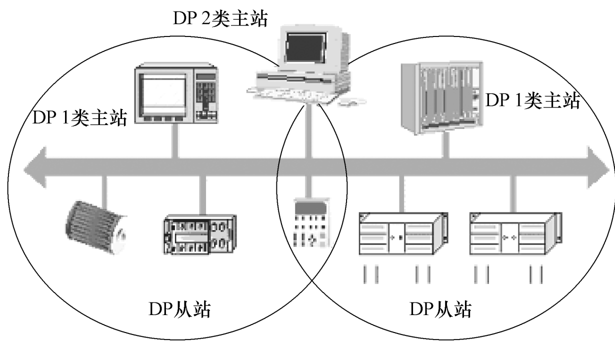


图 4-133 多主站系统

（3）纯主-主系统

网络站点都是主站。

从上述两图知，每个包括以下 3 种不同类型设备：

1）一级 DP 主站（DPM1）：一级 DP 主站是中央控制器，是必需的。它在预定的信息周期内与分散的站（如 DP 从站）交换信息。典型的 DPM1 如 PLC 或 PC。

2）二级 DP 主站（DPM2）：二级 DP 主站是编程器、组态设备或操作面板，在 DP 系统组态操作时使用，还可对系统进行操作和监视。

3）DP 从站：有 3 种：

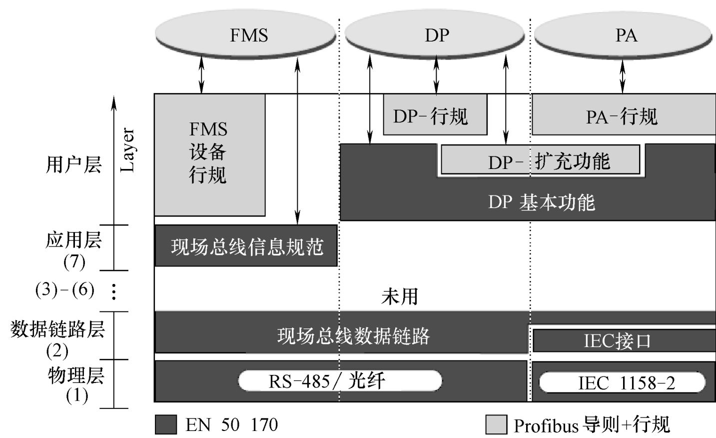
（a）PLC（智能型 I/O）：有 CPU 及内存，不能存储程序和执行程序，可存储程序和执行程序，自身有控制功能。同时有通信接口，可与主站通信，共享数据区。通过它，主站与它也能间接地相互控制。

（b）分散式 I/O（非智能型 I/O）：通常由电源部分、通信适配器部分、接线端子部分组成。分散式 I/O 没有 CPU 及内存，不能存储程序和执行程序，自身没有控制功能。通信适配器部分接收主站指令，按主站指令驱动 I/O，并将 I/O 输入及故障诊断等信息返回给主站。通常分散型 I /O 是由主站统一编址，这样在主站编程时使用分散式 I/O 与使用主站的 I/O 没有什么区别。

（c）驱动器、传感器、执行机构等现场设备：即带 Profibus 接口的现场设备，可由主站在线进行系统配置、参数修改、数据交换。至于那些参数可进行通信及参数格式由 Profibus 行规决定。

2. Profibus 协议结构

网络协议以 ISO/OSI 参考模型为基础，对第三～六层进行了简化，其协议结构如图 4-134所示。



注：第一层为物理层，第二层为数据链路层，第三～六层未使用，第七层为应用层。

图 4-134　Profibus 协议结构

从图知，这里不仅定义了 Profibus-DP 协议结构，还定义了 Profibus-FMS 及 Profibus-PA 协议结构。

Profibus-DP 定义了第一、二层和用户接口。OSI 的第三～七层未加描述。用户接口规定了用户及系统以及不同设备可调用的应用功能，并详细说明了各种不同 Profibus-DP 设备的设备行为。

Profibus-FMS 定义了第一、二、七层，应用层包括现场总线信息规范（Fieldbus Message Specification，FMS）和低层接口（Lower Layer Interface，LLI）。FMS 包括了应用协议并向用户提供了可广泛选用的强有力的通信服务。LLI 协调不同的通信关系并提供不依赖设备的第

二层访问接口。由于 DP 与 FMS 系统使用了同样的传输技术和统一的总线访问协议，因而这两套系统可在同一根电缆上同时操作。

（1）第一层，即物理层

其传输技术有 RS-485 及光纤。

1）RS-485。是 Profibus 最常用的一种传输技术。这种技术通常称之为 H2。采用的电缆是屏蔽双绞铜线。其技术基本特征：

（a）网络拓扑：线性总线，全部设备均与总线连接，两端有源的总线终端电阻，每个分段上最多可接 32 个站（主站或站）。

（b）传输速率：从 9.6kbit/s 到 12Mbit/s。电缆最大长度取决于传输速率。如使用 A 型电缆，则传输速率与传输距离对应关系见表 4-32 所示。

表 4-32　传输速率与传输距离对应关系

波特率/(kbit/s)	9.6	19.2	93.75	187.5	500	1500	1200
距离/段(M)	1200	1200	1200	1000	400	200	100

在一个有着 32 个站点的分布系统中，Profibus-DP 对所有站点传送 512 bit/s 输入和 512bit/s 输出，在 12Mbit/s 时只需 1ms。

（c）通信介质：屏蔽双绞电缆，也可取消屏蔽，取决于环境条件（EMC）。

（d）站点数：每分段 32 个站（不带中继），可多到 127 个站（带中继）。

（e）插头连接：最好使用 9 针 D 型插头。

（f）可通过中继器增加传输距离。当分段站超过 32 个时，必须使用中继器用以连接各总线段。串联的中继器一般不超过 3 个。中继器没有站地址，但被计算在每段的最多站数中。

2）光纤。当 Profibus 系统在电磁干扰很大的环境下应用时，可使用光纤导体，以增加高速传输的距离。可使用两种光纤导体，一是价格低廉的塑料纤维导体，供距离小于 50m 情况下使用。另一种是玻璃纤维导体，供距离大于 1km 情况下使用。许多厂商还提供有专用总线插头，可将 RS-485 信号转换成光纤导体信号或将光纤导体信号转换成 RS-485 信号。这使它的系统配置更加灵活、方便。

（2）第二层，称之为现场总线数据链路层（Fieldbus Data Link-FDL）

3 种 Profibus（DP、FMS、PA）均使用一致的协议。包括了保证数据可靠性技术及传输协议和报文处理。

介质存取控制（Medium Access Control-MAC）采用混合方式，即主站间按令牌方式，主站和从站间按主从方式。在主站之间按照地址的升序传递总线控制权（即令牌），得到令牌的主站才可发起通信。这可保证了在任一时刻只能有一个站点发送数据，可完全避免冲突；并且任一个主站在一个限定的时间内（Token Hold Time）都可以得到总线操作权。在这段时间内，主站可依照主-从通信关系表与所有从站通信，也可依照主-主通信关系表与所有主站通信。而从站没有总线控制权。

其特点还有，主站与从站可在任意时间接入或断开。总线访问协议（FDL）将自动重新组织令牌；令牌调度要确保主站有足够时间完成通信，为此如需要应做必要的计算；DP 从站有看门狗定时器（Watchdog Timer），对 DP 从站的输入/输出进行存取保护，而主站上有

可变定时器的用户数据传送监视，所以，协议有能力发现故障的站点、失效的令牌、重复的令牌、传输错误及可能的其他网络错误；可确保所有信息，包括令牌信息高度安全。此外，在总线系统初建时，主站介质存取控制 MAC 的任务是制定总线上的站点分配并建立逻辑环。在总线运行期间，断电或损坏的主站必须从环中排除，新上电的主站必须加入逻辑环。

第二层的另一重要工作任务是保证数据的无差错传输。具体是通过海明间距 =4、按照国际标准 IEC870—5—1 制定的特殊的起始和结束界定符、每个字节的奇偶校验和每个报文的 CRC 循环校验来保证。其最大报文长度为 255 个字节，所涵盖项目有：标识符、源及目的地址、数据长度、数据、命令字和循环校验码，最长有效数据为 246 字节。图 4-135所示为它的通信中请求及响应的过程。

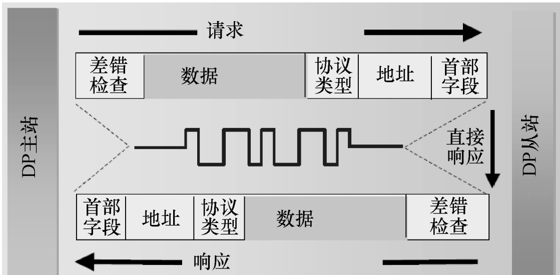


图 4-135　通信请求及响应过程

Profibus 链路层提供的服务有：SDA（发送数据并要求回答）、SDN（发送数据，不要求回答）、SRD（发送数据并要求回送数据）及 CSRD（循环发送数据并要求回送数据）。它按照非连接的模式操作，除提供点对点逻辑数据传输外，还提供多点通信，其中包括广播及有选择广播功能。

（3）应用层

Profibus 协议的第二部分是应用层协议（FMS），第三部分为 DP 协议，FMS 定义了应用层（第七层）的内容。由于 Profibus 没有第三～六层，所以这几层的必要功能在一个称为“底层接口”（LLI）的模块中完成，由 LLI 将这些功能映射到 FMS 中。FMS 提供了多种强有力的通信服务，这些服务是著名的 MAP 协议中 MMS 服务的一个子集。为使这些功能适应不同应用领域当中真正的实际需要，FMS 包括称为“行规”（Profile）的特殊定义。行规规定不同制造商制造的、遵从同一行规的 Prifibus 设备应具有相同的通信功能。行规中除通信参数的选择外，还包括对状态和错误的解释及针对应用的定义等许多内容。

Profibus 已纳入国际 IEC 61158 及我们国家 JB/T 10308. 3-2001 标准。还有很多细节，可直接从中了解。

3. Profibus-DP 功能

有基本功能及扩展功能，有 3 种版本对此做了规定。基本功能由（版本 DP-V0）来规定。特殊需求的扩展功能由 DP-V1 和 DP-V2 规定。版本的这种区分，主要反映了由于不断增长的应用需求所编订的规范时间顺序。版本 V0 和 V1 包含“特性”（用于实现的绑定）和选项，而 V2 仅规定了选项。3 种版本的主要内容如下：

DP-V0 提供 DP 基本功能，包括循环的数据交换，以及站诊断、模块诊断和特定通道的诊断。表 4-33 列出了 DP-V0 的功能概况。

DP-V1 包含依据过程自动化的需求而增加的功能，特别是用于参数赋值、操作、智能现场设备的可视化和报警处理等（类似于循环的用户数据通信）的非循环的数据通信。这样就允许用工程工具在线访问站。此外，DP-V1 有 3 种附加的报警类型：状态报警，刷新报警和制造商专用的报警。

表 4-33 DP-V0 功能概况

总线存取	· 主站之间的令牌传送程序和主站与从站之间的数据传送 · 单主站或多主站系统，可选 · 在一条总线上，最多可接 126 个主站和从站设备
通信	· 点对点(用户数据通信)或群播(控制命令) · 循环的主站-从站用户数据通信
运行状态	· 运行 循环地传输输入和输出数据 · 清除 读输入，输出保持在故障安全状态 · 停止 诊断和参数分配，无用户数据传输
同步	· 控制命令能使输入和输出同步 · Sync mode 同步输出 · Freeze mode 同步输入
功能	· DP 主站与多个从站之间的循环用户数据传输 · 动态的激活/解除激活各个从站；检查从站组态 · 强有力的诊断功能，3 级诊断报文 · 输入和/或输出的同步 · 通过总线对从站分配地址，可选的 · 每个从站的输入/输出数据最多 244B
保护功能	· 报文传输的海明距离：HD = 4 · DP 从站的监视器控制检测指定的主站故障 · 对从站的输入和输出的存取保护 · 用主站中可调节的监视定时器来监视用户数据通信
设备类型	· 1 类 DP 主站(DPM1)，中央可编程序的控制器，如 PLC，PC · 2 类 DP 主站(DPM2)，如工程或诊断工具 · DP 从站，如二进制的或模拟的输入/输出设备，驱动器，阀门等

DP-V2 包括主要根据驱动技术的需求而增加的其他功能。由于增加的功能，如同步从站模式（Isochronous Slave Mode）和从站对从站通信（Data eXchange Broadcast，DXB）等，DP-V2 也可以被实现为驱动总线，用于控制驱动轴的快速运动时序。

DP 的各种版本功能在 IEC 61158 中都有详细说明。这里不再赘述。

4. Profibus-DP 特点

1）代替 PLC/PC 与 I/O 之间昂贵的电线。

2）快速传输，1KB 的输入数据和 1KB 的输出数据所需时间 <2ms。

3）强有力的工具减少组态和维护费用。

4）被所有主要的 PLC 制造商支持。

5）有广泛的产品：PLC、PC、I/O、驱动器、阀、编码器等。

6）允许周期性和非周期性的数据传输。

7）单主和多主网络。

8）每个站的输入和输出数据量大，最多可达 244B。

4.5.2 西门子 PLC Profibus 组件及配置实例

1. 西门子组件

（1）一类主站

选择 PLC 做一类主站。有两种形式：

1）处理器CPU带内置Profibus接口。这种CPU具有“DP”的CPU至少有一个DP接口，如315-2PN/DP和317CPU配有一个MPI/DP接口。CPU319-3PN/DP具有一个MPI/DP接口和一个附加的DP接口。带有MPI/DP接口的CPU带有缺省的MPI组态。如果要使用DP接口，则需要在STEP7中设置DP模式。

2）Profibus通信处理器。CPU不带Profibus接口，需要配置Profibus通信处理器模块。具体见表4-34所示。

表4-34 Profibus通信处理器及其功能

型　　别	功　　能
S7-300 CP 342-5： CP 342-5 FO(集成光纤接口) CP 343-5：	连接SIMATIC S7-300系列PLC到Profibus网络，或扩展PLC的通信处理能力 通过独立的通信处理器减轻了主CPU的通信任务，提高了通信效率和可靠性
S7-400 CP 443-5基本型： CP 443-5扩展型： IM 467： IM 467-FO(集成光纤接口)	连接SIMATIC S7-400系列PLC到Profibus网络，或扩展PLC的通信处理能力 通过独立的通信处理器减轻了主CPU的通信任务，提高了通信效率和可靠性 CP 443-5支持冗余的总线拓扑结构

（2）二类主站

有PC/PG加各种网卡及运行相应系统与网络软件。有：

1）CP5411、CP5511、CP5611网卡。自身不带微处理器，可运行多种软件包，9针D型插头可成为Profibus－DP或MPI接口。CP5411是短ISA卡。CP5511是TYPEⅡ PCMCIA卡。CP5611是短PCI卡。

2）CP5412通信处理器。用于PG或AT兼容机，ISA总线卡，9针D型接口。具有DOS、WIN3.11、WIN95、WIN NT及UNIX操作系统下的驱动软件包。支持FMS、DP、FDL、S7及PG功能。具有C语言接口（C库或DLL）。数据传输速率：9.6kbit/s、12Mbit/s。

（3）从站组件

有分布是I/O、智能从站等。

1）分布式I/O。用于S7系列的产品主要有：

（a）ET200M。是一种模块式结构的远程I/O站。由IM153 Profibus-DP接口模块、电源、各种I/O模块组成。可使用S7-300系列所有I/O模块，如SM321/322/323/331/332/334. EX. FM350-1/351/352/353/354等。最多可扩展到8个I/O模块。最多可提供的I/O地址为：128字节输入/128字节输出。防护等级IP20。最大数据传输速率为12Mbit/s。具有集中和分散式的诊断数据分析。

（b）ET200 L。是小型固定式I/O站。由端子模块和电子模块组成。端子模块含有电源及接线端子。电子模块含有通信部分及各种类型的I/O。可选择多种DC24V开关量输入。输出及混合输入/输出模块。如16DI、16DO、32DI、32DO、16DI及16DO等。具有集成的Profibus-DP接口。防护等级IP20。最大数据传输速率：1.5Mbit/s。具有集中和分散式的诊断数据分析。

再 ET200L-SC 是可扩展的 ET200L，由 TB16SC 扩展端子，可扩展 16 个 I/O 通道。这 16 个通道可按 8 组自由组态。即由几个微型 I/O 模型组成。每一个微型 I/O 模块可以是 2DI、2DO、1AI 及 1AO。

（c）ET200B。是小型固定式 I/O 站。由端子模块和电子模块组成。端子模块含有电源. 通信口及接线端子。电子模块含有各种类型的 I/O。有各种 DC24V 螺丝端子模块。有 DC24V 弹簧子模块。120V/230VAC 螺丝端子模块及用于模拟量的弹簧端子模块。有多种 DC24V 开关量输入。输出及混合输入/输出模块，包括：16DI、32DI、16DO、32DO、24DI/8DO、16DI/16DO、8RO 及 8DI/8DO。有各种 AC120/230V 开关量输入、输出及混合输入/输出模块，包括：16DI、32DI、16DO、16RO、8DI/8RO 及 32DO。有各种模拟量输入输出及混合输入/输出模块，包括：4/8AI、4AI 及 4AO。具有集成的 Profibus－DP 接口。防护等级 IP20。最大数据传输速率：12Mbit/s。具有集中和分散式的诊断数据分析。

（d）ET200 C。是小型固定 I/O 站。具有高防护等级 IP66/67，“UL50，TYPE 4”认证。具有集成的 Profibus-DP 接口。有多种 DC24V 开关量输入。输出及混合输入/输出模块，包括：8DI、8DO 及 16DI/16DO。有多种模拟量输入输出及混合输入/输出模块，包括：4/8AI、4AI 及 4AO。最大数据传输速率：开关量输入/输出时 12Mbit/s，模拟量输入/输出时 1.5Mbit/s。

（e）ET200X。是一种坚固型结构的分散式 I/O 站。设计保护等级为 IP65。模块化结构。由一个基本模块和若干扩展模块组成。最多可扩展 7 个扩展模块。有两种基本模块：8DI/24VDC 及 4DO/24VDC/2A。而扩展模块有：4DI/24VDC、8DI/24VDC、4DO/24VDC/2A、4DO/24VDC/0.5A、2AI/±10V、2AI/±20mA、2AI/420mA、2AI/RTD/PT100、2AO/±10V、2AO/±20mA 及 2AO/420mA。

2）智能从站。主要是 EM277。用于使 S7-200 作为从站接入 Profibus 网络。图 4-136 所示为它的外观。

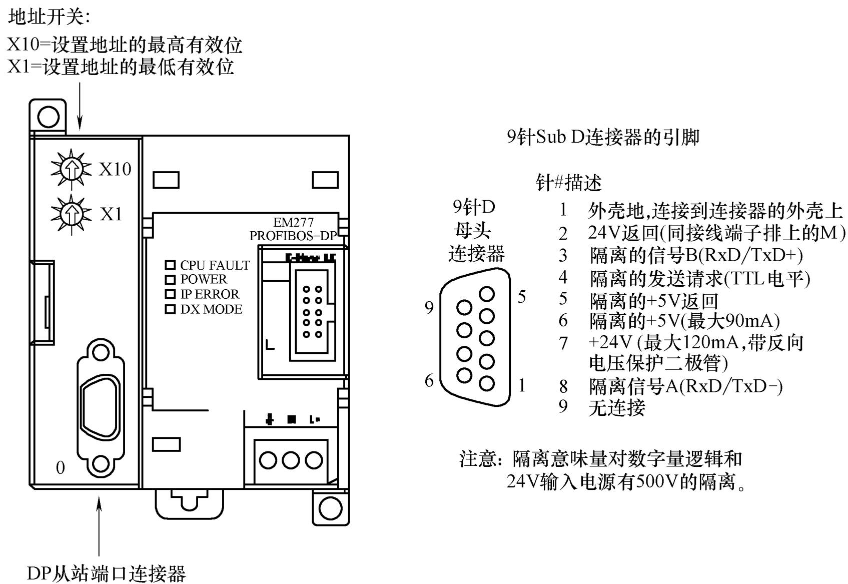


图 4-136　EM277 模块外观

EM277 是智能模块，其通信速率为自适应。在 S7-200 CPU 中不用做任何关于 Profibus-DP 的配置和编程工作，只需做好对数据的处理。Profibus-DP 的所有配置工作由主站完成。在主站中需配置从站地址及 I/O 配置。EM277 作为一个特殊的 Profibus-DP 从站模块，其相关参数（包括上述的数据一致性）是以 GSD（或 GSE）文件的形式保存的。在主站中配置 EM277，需要安装相关的 GSD 文件。

（3）通信介质、网络附件及相关软件

西门子提供有成套产品。具体可参阅有关产品目录。

附带提及的是 Profibus 还允许第 3 方产品接入。但它得提供的 GSD 文件。将 GSD 文件加载到 STEP 7 等软件指定目录下，使用 STEP 7 等软件才可在该界面下进行第三方产品在系统中的配置。

2. 西门子 Profibus 配置实例

（1） S7400 通过 Profibus-DP 连接 ET200M。本例组态过程如下：

1）运行 S7 编程软件，建立新建项目“S7400-ET200M”，插入 S7 CPU412-2DP。结果如图 4-137所示。

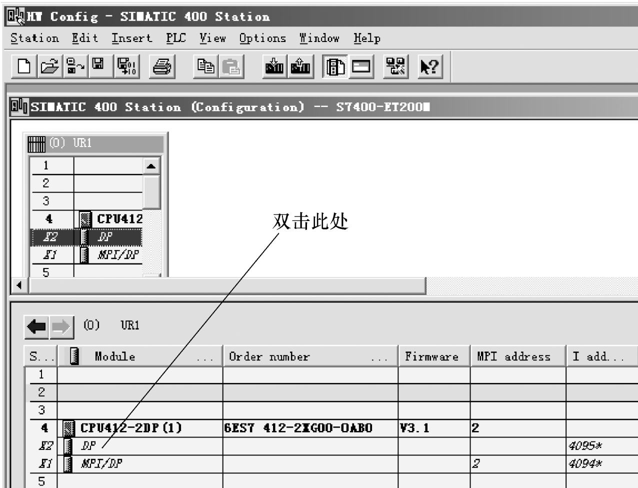


图 4-137　插入 CPU412-2DP（1）模块

2）双击图 4-137 所示槽架中的 DP 项，将弹出如图 4-138 所示“Properties-DP”对话框。

本例在“工作模式”标签中选定为 DP 主站。在“General”标签中点击“属性”，还可更改站点的地址。本例站点地址设置为 2。完成设置后点击“确定”。意味着网络已建立。但如图 4-139 所示只是仅有主站的网络。

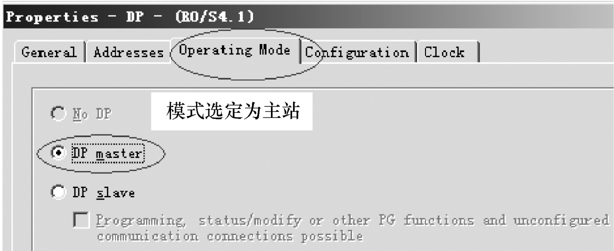


图 4-138　属性-DP 对话框

3）在仅有主站的网络上添加从站。办法如图 4-140 所示，先拖放 IM 153 接口模块到“拖放到此”处。组态好的 DP 系统中挂上 ET200M 从站，同时会弹出“属性-Profibus”对话框，此时可点“Cancel”过后再设置 ET200M 的属性。

4）双击组态好的 ET200M 图标，出现如图 4-141 所示“DP slave Properties（DP 从站属性）”

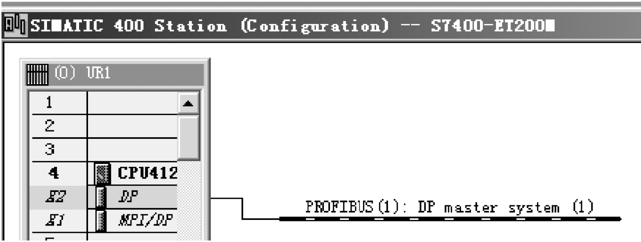


图 4-139　仅有主站的网络

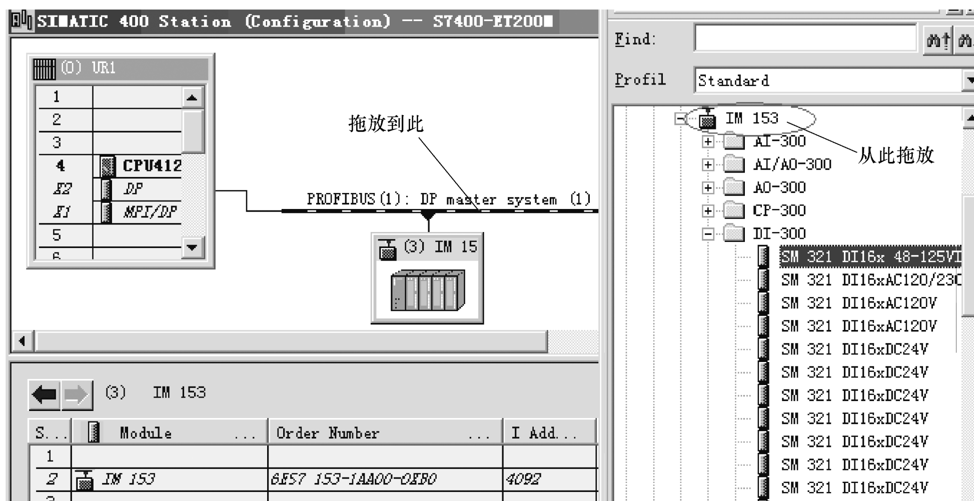


图 4-140　拖放 IM153-1 到 “DP 图”

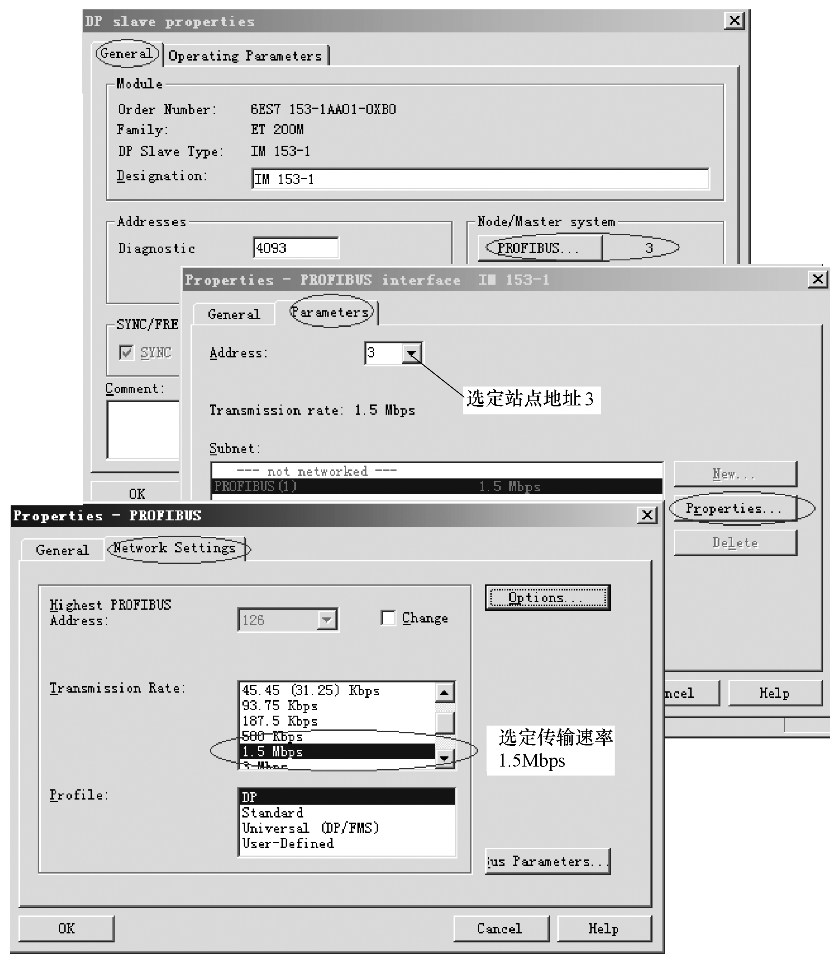


图 4-141　DP slave Properties 等一组窗口

对话框。之后再点击其上“Profibus”，将弹出“Properties-Profibus interface IM 153-1”窗口。本例从中选定站点地址为 3（注意设定地址须和 ET200M 硬件上拨码数字相同，且不能和其他站冲突）。接着点击其上的“Properties”按钮。进而弹出“Properties-Profibus”窗口。本例从中选定传输速率为 1.5Mbit/s。

选定后逐一点击相继窗口上的“OK”按钮。则完成了从站 IM 153-1 接口的组态。

5）组态 ET200M 的硬件 I/O。这时可以根据需要从 IM153-1 栏下进行硬件组态，如：AI 是模拟量输入，DI/DO 是开关量输入输出等。加入的方法也是拖放。如图 4-142 所示，本例 ET200M 硬件组态是，加入 16 点直流输入（图示已加入）及正加入的 16 点交流输出。还可看出输入地址（I Addresses）是 IB0、IB1，是软件自动加入的。输出地址（Q Addresses）是 QB0、QB1，也是软件自动加入的。

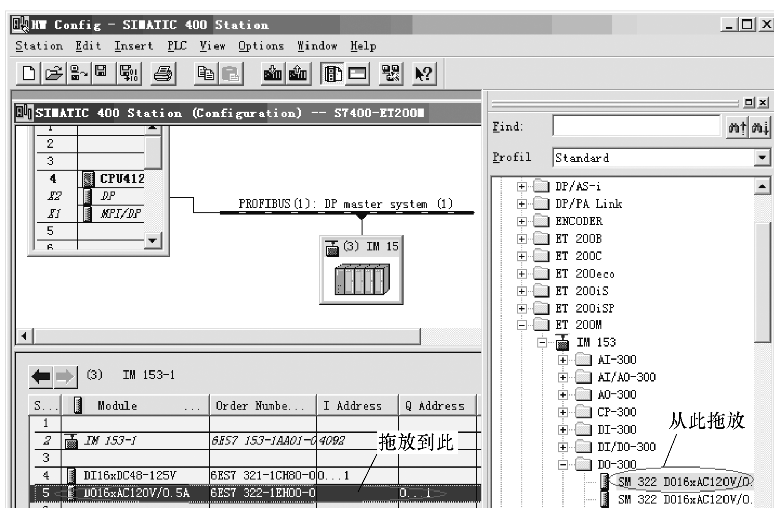


图 4-142　ET200M 硬件组态

当然这个 IQ 地址也可更改。办法是，双击所要改的已加入的模块。如双击“DixDC48-125V”模块，将弹出如图 4-143 所示的“Properties-DixDC48-125V”窗口。可在“Addresses”表单下的“Inputs”项下更改“Start”值。只是要确保所编辑的地址不能与当地的 I/O 地址及其他分布 I/O 地址重复。

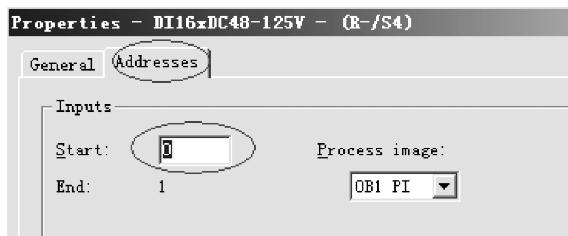


图 4-143　Properties-DixDC48-125V 窗口

完成上述组态，S7-400 的 CPU 控制这远程 I/O 与处理本地 I/O 本质上没有区别。所差的只是通信延迟。

本例介绍的主站是 S7-400。其实，S7-300 也一样可以用。从站用的 ET200M，其他的也当然可用。而且，还可增加更多的从站。其组态的方法与这里介绍的完全一样。

（2）S7-200 与 S7-300 通过 Profibus 连网实例

为此，须在 STEP7 中对 S7-300 站组态；而 S7-200 不须组态。有关 S7-300 组态过程如下：

1）与上述 S7-400 通过 Profibus-DP 连接 ET200M 组态实例一样，先建立仅含有 S7-300 主站的 Profibus 的网络。

2）安装 EM277 从站配置文件。办法是，点击 STEP7 的硬件组态窗口主菜“Option”项下的“Install new GSD”项，以导入 SIEM089D. GSD 文件，如图 4-144 所示。

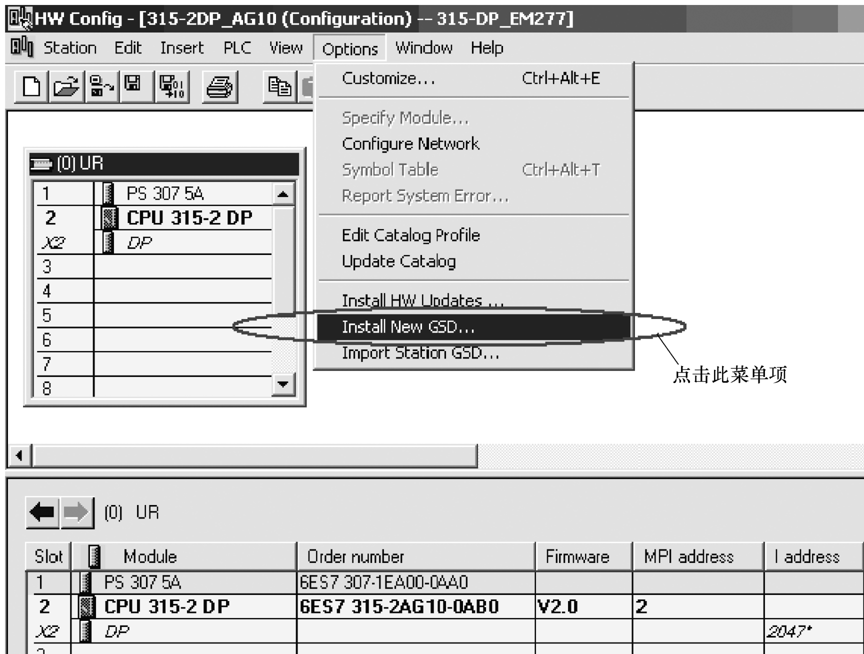


图 4-144 点击“Install new GSD”项

3）在弹出如图 4-145 所示的“Installing new GSD”窗口的“SIMATIC”文件夹中，选中 EM277 的 GSD 文件（SIEM089D. GSD），并点击“Open”按钮即可导入该文件。如果找不到这个文件可上网搜索、下载。并在下载存储的目录中找出它。

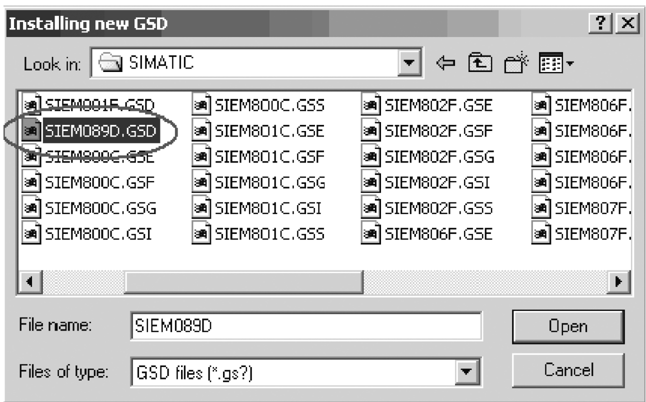


图 4-145 Installing new GSD 窗口

4）导入 GSD 文件后，在“HW Config”窗口右侧的设备选择列表的“Profibus DP”→（下的）“Additional Field Devices”→（下的）“PLC”→（下的）“SIMATIC”→（下的）“EM277”以及下的诸项。这时还是用拖放方法，办法如图 4-146 所示，先把“EM277”拖放到所建的仅有主站的网络上。之后会弹出“Properties Profibus Interface EM277 Profibus-DP”窗口，从中可选定从站地址。还可从中点击“Properties”按钮，进而做相应选定。但此时“EM-277 Profibus”下仍为空。表示仍需指定实际的 I/O 点数。

5）为此，可根据需要选择一种 I/O 点数。本例中选用了如图 4-147 所示为 8 字节输入/

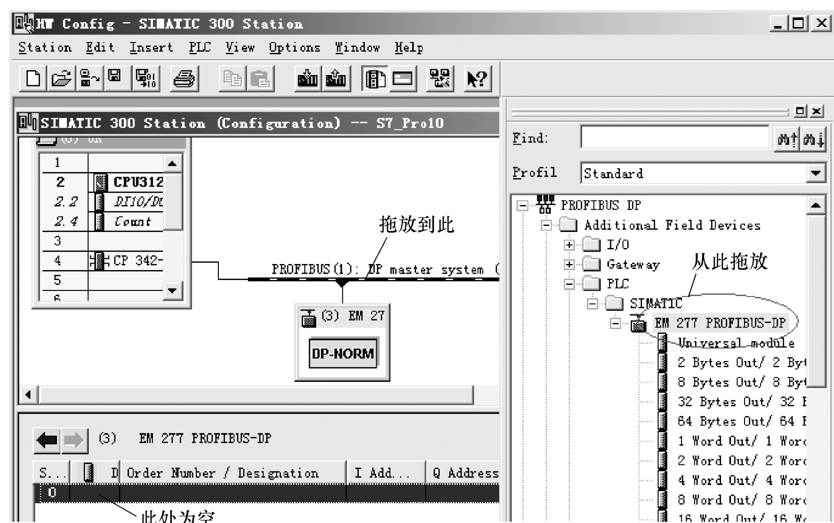


图 4-146　把“EM277”拖放到网络上

8 字节输出。

6）根据 EM277 上的拨位开关设定以上 EM277 从站的站地址，如图 4-148 所示。但此地址应与上述软件设置的地址一致。

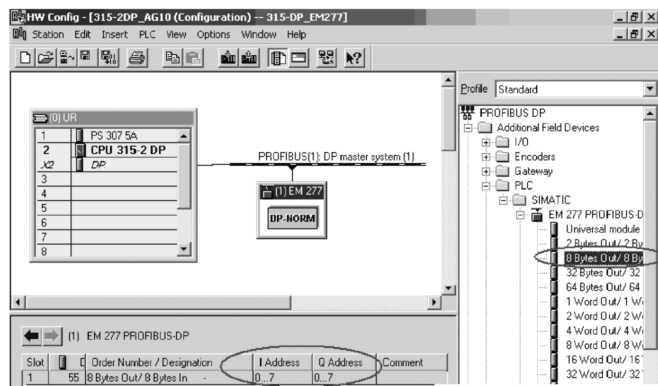


图 4-147　选用 8 字节输入、8 字节输出

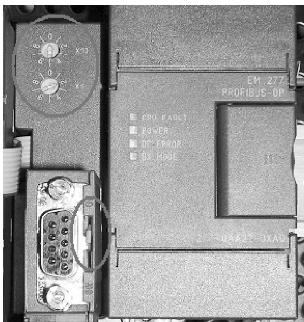


图 4-148　硬件设定 EM277 从站地址

7）组态完系统的硬件配置后，存盘并将硬件信息下载到 S7-300 的 PLC 当中。这样，在 S7-200 中的 VB0 ~ VB15 将对应到 S7-300 的 PQB0 ~ PQB7 和 PIB0 ~ PIB7。也就是，VB0 ~ VB7 是 S7-300 写到 S7-200 的数据，VB8 ~ VB15 是 S7-300 从 S7-200 读取的值。

有了上述组态，两个主从 PLC 即可进行数据交换。而如何准备与使用这些交换数据那是通信编程的任务，这里略。

（3）S7-400 为主站而 S7-300 为从站的配置实例

一般，此种情况下先配置从站。具体步骤是：

1）建立“S7-300 从站”项目，插入 S7-300 站。再双击“硬件”，进入如图 4-149 所示的“HW Config”（硬件组态）环境（本例 Step7 为中文界面）。

2）在硬件组态环境中，如图 4-150 所示，依次放入机架，电源模块和 CPU 模块。



图 4-149 HW Config 环境



图 4-150 依次放入机架，电源模块和 CPU 模块

3）在放入 CPU 模块时，会出现如图 4-151 所示的“属性-Profibus 接口”对话框，选择 S7-300 从站的地址。点击“属性”可以修改传输的波特率。

4）此时如图 4-152 所示，所组态的 S7-300 还是 DP 主站。

5）为此，要双击槽架中的 DP 项目，出现如图 4-153 所示的“属性-DP”对话框，在“工作模式”标签中改为“DP 从站”。并点击“确定”完成更改。



图 4-151 属性-Profibus 接口对话框

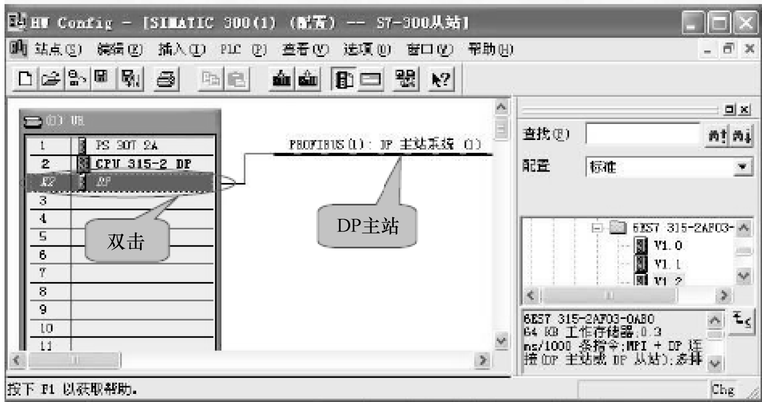


图 4-152 所组态的 S7-300 还是 DP 主站

6）这时，组态为从站后的状态如图4-154所示。

7）点击第5步图示中的“组态”标签。将出现如图4-155所示 DP 组态表单。

8）点击该窗口上的“新建”按钮，将弹出如图4-156所示的组态窗口。在其上刻组态 S7-300 的数据接收和发送区。

9）点击“确定”，完成从站组态。如图4-157所示转到地址表单，可以看出，本例从站 S7-300 的输入是 IB0，输出是 QB0。

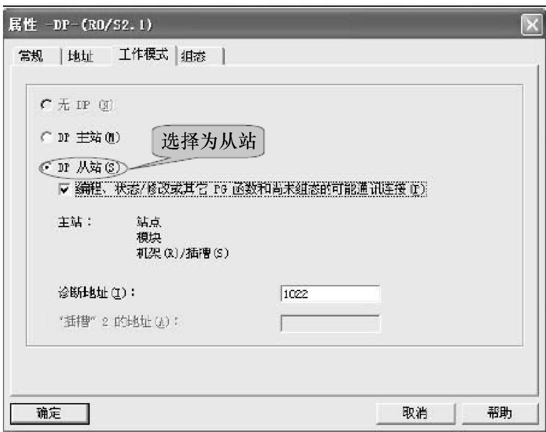


图4-153 属性–DP 对话框



图4-154 组态为从站后的状态



图4-155 DP 组态窗口



图 4-156　弹出组态窗口



图 4-157　从站 S7-300 输入、输出

10）以下也是用同样方法进行 S7-400 组态。只是选择 S7-400 为 DP 主站。组态完成后出现仅有 S7-400 主站的网络如图 4-158 所示。

11）如图 4-159 所示，在 S7-400 的 HW configuration 组态界面右侧，选择 Profibus DP 下的“Configured Stations”中的 CPU31x，将其拖放到左侧的 Profibus 总线上。

12）从站拖放完成后，会自动弹出如图 4-160 所示的“DP 从站属性”对话框。在它的“连接”表单上，会显示已经组态好的从站信息，选中一个站点，再点击“连接”即可激活该连接。本例仅有一个从站 CPU315。

13）激活连接后将显示如图 4-161 所示的连接的信息。当然，也可以重新断开连接，那意味着它不再是 S7-400 的从站。这当然不是本例的含义，所以不这么做。



图 4-158　仅有 S7-400 主站的网络

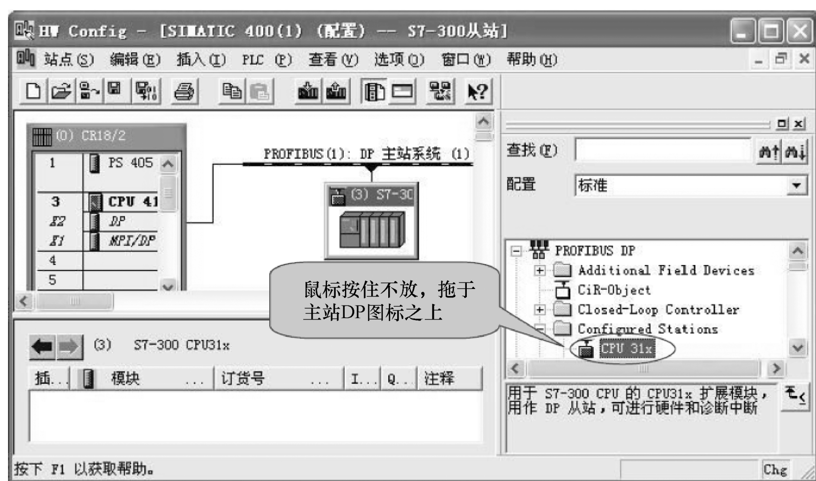


图 4-159　把从站 S7-300 拖放在网络上

14）点击“组态”标签，将出现如图 4-162 所示 DP 组态表单。可在其上组态主站的发送和接收区。

15）选中第一行，先组态主站的发送区（对应从站的接收区），再点击“编辑”按钮，将弹出如图 4-163 所示的“DP 从站属性”窗口，可从中选定主站的地址类型（和从站相对应）和地址。

16）同样，组态 S7-400 的接收区。组态完成后的画面如图 4-164 所示。

从图可看出，S7-400 主站和从站 S7-300 通信数据区的关系是：S7-400（主站）的输出是 QB0，而对应的 S7-300（从站）输入为 IB0；S7-400（主站）的输入是 IB0，而对应的 S7-300（从站）输出 QB0。

最后，把组态存盘并下载到 CPU 中去，然后就可以在主站和从站中通过交换数据区分别读取对方的数据了。



图 4-160　DP 从站属性对话框



图 4-161　完成的连接信息



图 4-162　DP 组态表单



图 4-163　DP 从站属性窗口

（4）Profibus-DP DX（Direct Data exchange，直接数据交换）方式及其通信组态实例。

图 4-165 所示的 MS 方式与 DX 方式通信示意。从图可看出，DX 模式是 MS 的补充。有了它，在主站轮询从站读取数据时，从站广播发送数据给主站的同时，也发送给指定从站。这样发送数据的从站称为“Publisher”，也接收这样发送数据的从站称为“Recipient”。本例将介绍 DX 模式通信组态。

主站为 S7-400 CPU414-3DP。两个从站分别为 S7-300 CPU315-2DP 和 CPU314C-2DP。其组态过程先是，新建一个项目，将该实例起名为 Profibus_ DP_ DX，具体组态由从站开

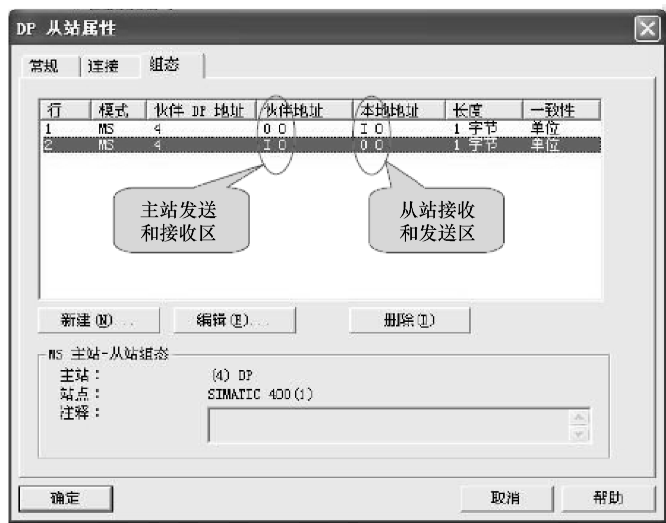


图 4-164　S7-400 接收区组态完成图面

始，只是本例与上例不同，用的是英文界面：

1）组态两个 S7-300 从站，过程同上例从站组态。CPU315 – 2DP Profibus 地址为 3，CPU314 – 2DP Profibus 地址为 4。“Operating Mode”（操作模式）都选择从站模式。点击“Properties”在“Network setting”中设置传输速率和总线行规，这两个站点都选择“ DP ”行规，传输速率选择“1.5Mbit/s”。如网络中使用了中继器、OBT 和 OLM 等网络元件，可点击“Option”按钮添加，然后点击“OK”按钮确认。

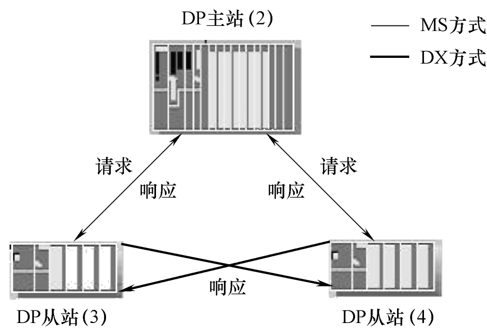


图 4-165　MS 与 DX 方式通信示意

2）点击“Cofiguration”标签，进入如图 4-166 所示的“Cofiguration”表单窗口。

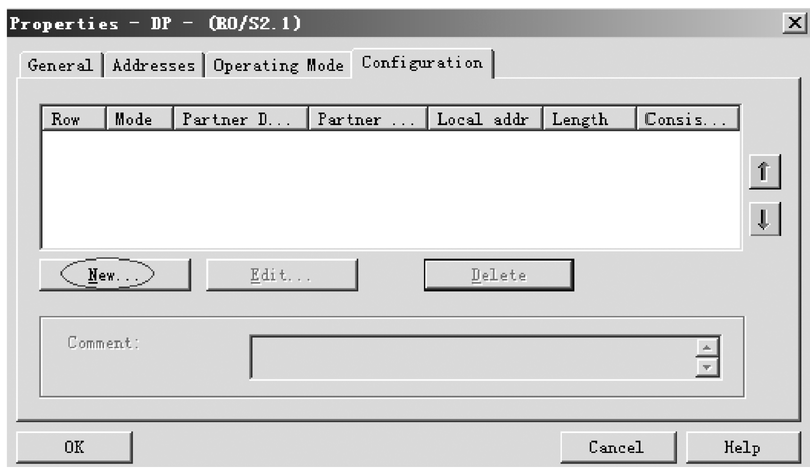


图 4-166　Cofiguration 表单

3）在此窗口上，点击“New”按钮，将弹出如图 4-167 所示的“Properties-DP Cofiguration ROW 1”配置窗口。

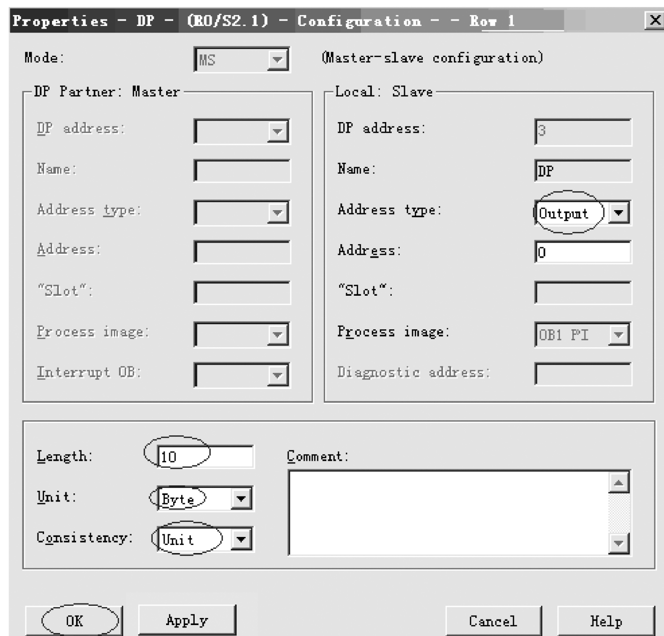


图 4-167　所示的“Properties-DP Cofiguration ROW 1”配置窗口

4）在其上可进入 ROW 1 组态。本例选择 Address Type（地址类型）为 Output（输出），Length（长度）为 10 字节，Address（开始地址）为 0。还有其他选项可做相应选择。完成后点击“OK”按钮。将关闭此窗口。回到图 4-166 所示画面。但这时如图 4-168 所示，在它的 ROW 1 添加有所配置的输出项。

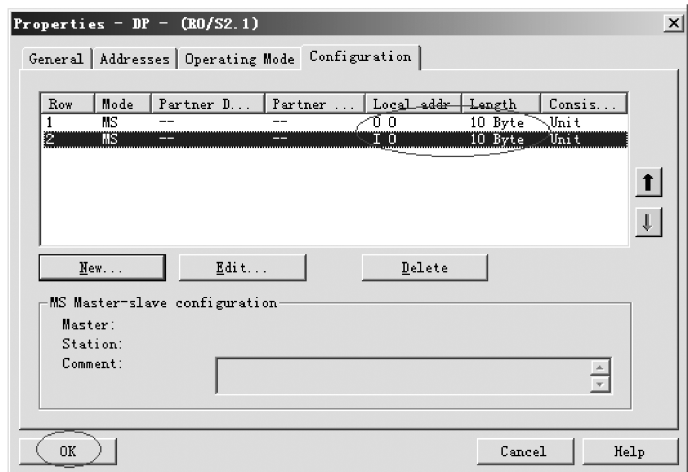


图 4-168　ROW 1 已添加输出项

5）从图知，它的 ROW 2 添加有输入项。办法与在 ROW1 添加输出项相同。也是先点击 4-1 的“New”按钮。之后所不同的是，它选择 Address Type 为输入。接着还可添加。本例只添加两行。

6）接着点击图 4-168 上的“OK”按钮。关闭此窗口，完成从站组态。

7）组态 S7-400 主站。过程与组态从站基本相同，只是它的操作模式选“主站”。结果如图 4-169 所示，就是只有主站的网络。

8）在 S7-400 的 HW configuration 组态界面右侧选择 Profibus DP。在如图 4-170 所示的“Configured Stations”中选择 CPU31x，将其拖放到左侧的 Profibus 总线上。

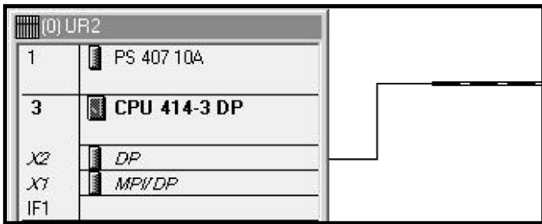


图 4-169 只有主站的网络

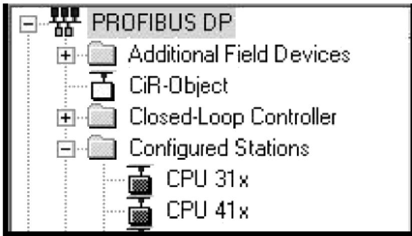


图 4-170 选择 CPU31x

9）拖放后将弹出 DP slave properties 对话框。出现已经组态的两个从站，如图 4-171 所示。

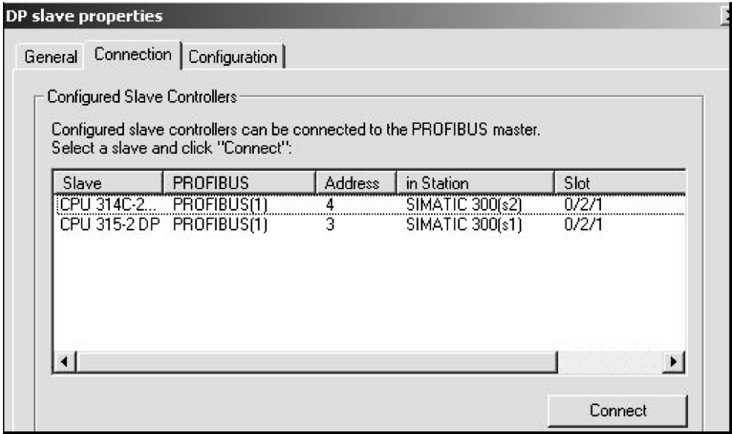


图 4-171 DP slave properties 对话框

10）选择其中一个 CPU，点击“Connect”，将其连接到 Profibus 网络。然后以同样的方法连接另一个从站。若要从网络上断相开关站点，可选择“Disconnect”。

11）连接完成后要为两个 S7-300 从站设置其对应主站输入输出接口区。例如，要设置地址为 3 的 CPU315－2DP 的输入输出接口区，可双击 3 号站，在弹出如图 4-172 所示的 DP slave properties 中的“Configuration”表单中，点击键“Edit”以组态主站即 CPU414－3DP 的通信接口区。

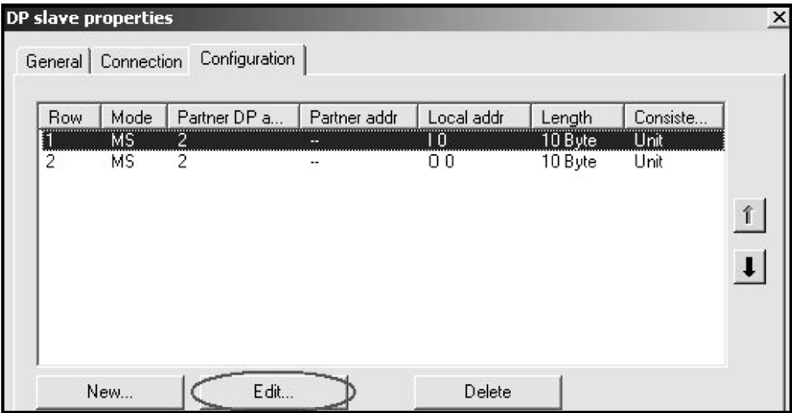


图 4-172 DP slave properties Configuration 表单

12）分别组态主站的通信地址区。对应规则为主站输出对从站输入，主站输入对从站输出。然后以同样的方法组态 4 号从站对应主站的通信接口区。组态完成后对应的地址关系如图 4-173 所示。

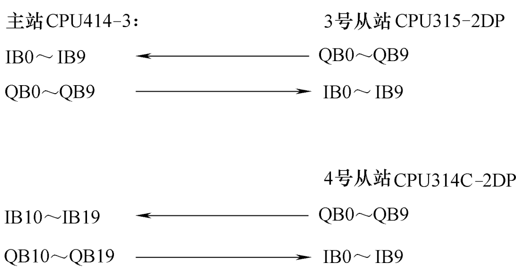


图 4-173　主从站对应地址关系

13）组态 DX 通信区。以上组态为 Profibus－DP MS 通信模式，完成后可进行 DX 模式组态。以下以 3 号从站作为“Publisher”，以 4 号从站作为“Recipient”为例说明 DX 模式通信组态。过程为：双击 4 号从站图标，在弹出如图 4-174 所示的窗口上，“Mode”选择 DX 模式，“Publisher”地址选择 3 号站。在下面的选择中要注意：“Publisher”的“Address type”为“ Input”，“Address”可选择，这里都是指“Publisher”对应主站的“Address type”和“Input”，从图 4-173 可以看到 3 号站发送给主站数据对应主站的接收区为 IB0～IB9。如果在“ Input”区选择 0，则“ Recipient”4 号从站将接收主站地址 IB0～IB9 也就是 3 号从站“Publisher”QB0～QB9 的数据，如果选择 4，则接收 3 号从站“Publisher” QB4～QB9 的数据，也就是说“Recipient”

可以有选择地接收“Publisher”地数据。参数组态如图 4-174 所示。

从上面地对应关系可以看到，当主站轮寻 3 号从站时，3 号从站发送 QB0～QB9 到主站 IB0～IB9 中，同时发送 QB4～QB9 6 个字节到 4 号从站 IB10～IB15 中，这里容易弄混淆的地方就是“Publisher”的地址区，站地址是从站地址，通信区却是主站的。

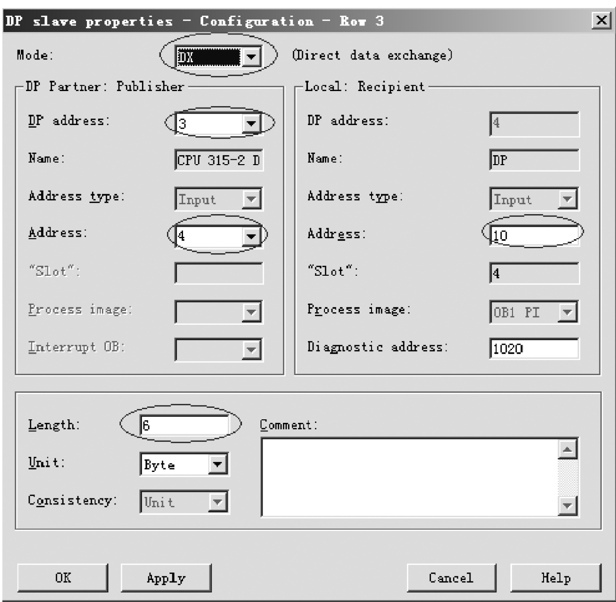


图 4-174　从站 4 DX 模式组态

其实本例也可对 3 号从站做上述组态。这时 4 号从站为发送者，3 号从站为接收者。方法类似，具体组态略。

（5）Profibus-DP DX 模式的多主讯通信组态实例

主要站点分布如图 4-175 所示。

从图 4-178 中可以看到，3 号从站（S7300 CPU314C-2DP）的一类主站为 2 号站（S7-400 CPU414-3DP），4 号站（S7-300 CPU315-2DP）为在同一 Profibus 网络上其他从站的主站。4 号站当然也有从站，这里略。本例组态要求是实现从站 3 与非它的主站 4 之间 DX 通信。即当 2 号主站轮询 3 号从站时，3 号从站的数据发送到 2 号主站的同时，还可以发送给 4 号主站。而 4 号主站可以选择接收数据的长度。本例组态与上例所差的只是 4 号站现在是主站，其他均相同。所以，相同部分的组态完全一样。这里不再重复。以

下仅对不同部分作简要说明：

双击上图中的 DP 栏，选择操作模式为“ Master ”，选择“Configuration”栏，点击键“New”，组态 4 号主站与 3 号从站的通信接口区，与 DX 通信一样，这时的通信模式以变为“DX”模式，主站轮询从站读取数据时，从站广播发送数据给其一类主站和其他主站，那么这个从站称为“Publisher”，接收数据的其他主站称为“Recipient”，由于上面组态的从站是 3 号站，那么 3 号从站将作为“Publisher”，4 号主站作为“Recipient”，如图 4-176 所示。

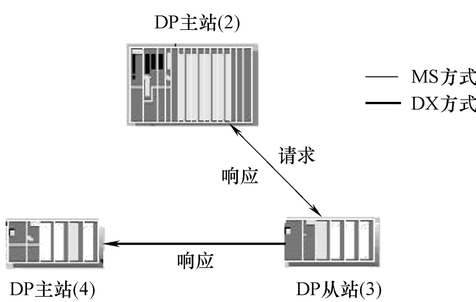


图 4-175　DX 模式的多主讯通信

在下面的选择中要注意：“Publisher”的“Address type”为“Input”，“Address”可选择，这里都是指“Publisher”对应其一类主站的“Address type”和“Input”，从上面组态可以知道 3 号从站发送给主站数据对应主站的接收区为 IB0 ~ IB9。如果在“Input”区选择 0 ，则“Recipient”4 号从站将接收主站地址 IB0 ~ IB9 也就是 3 号从站“Publisher”QB0 ~ QB9 的数据，如果选择 4 ，则接收 3 号从站“Publisher”QB4 ~ QB9 的数据，也就是说“Recipient”可以有选择地接收“Publisher”的数据，本例中选择 4 号主站的接收区为 IB0 ~ IB9，对应于 3 号从站的数据发送区为 QB0 ~ QB9。如果所有通信数据区，在上面例子中“Publisher”为智能从站（带有 CPU），普通的从站如 ET200M 等也可以作为“Publisher”，“Recipient”可以是多个，多主通信时，只有从站的一类主站可以发送数据给其从站，其他主站不能给作为“Publisher”的从站发送数据，只能接收数据。

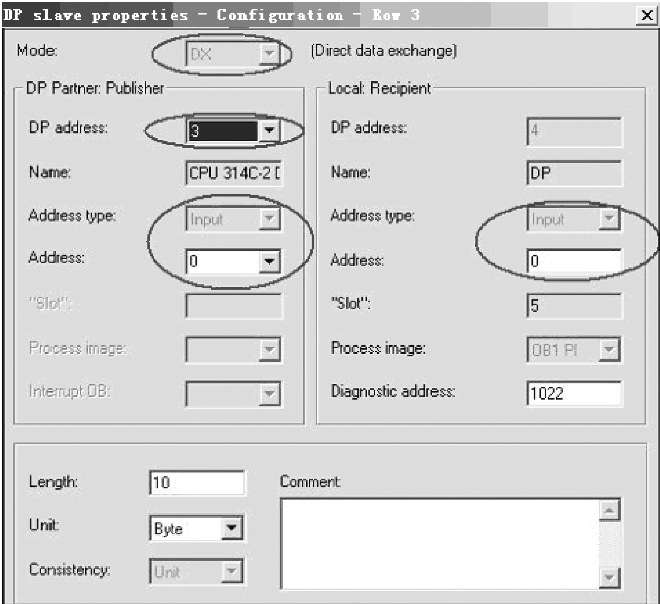


图 4-176　从站特性组态

4.5.3　和利时 PLC Profibus 组件及配置实例

和利时小型机 LEC G3 配置有 Profibus-DP LM3401 模块，可用以把 LEC G3 系列 PLC 作为从站，接入 Profibus-DP 网络。但进行硬件安装时，应放在紧随 CPU 模块右侧的第一个位置，如图 4-177所示。

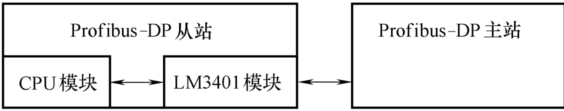


图 4-177　LM3401 模块的网络功能图

1. LM3401 模块功能、特性、接线及硬件设定

LM3401 模块的通信功能见表 4-35，物理特性见表 4-36，指示灯的状态描述见表 4-37。

表 4-35　LM3401 模块通信功能

名　称	功 能 描 述
通信口数量	1 个
接口类型	9 针 D 型孔座及接线端子
隔离耐压	1500V(AC)
Profibus-DP 波特率	9.6、19.2、45.45、93.75、187.5、500kbit/s 和 1、1.5、3、6、12Mbit/s(自适应)
站地址设定	0~126(由拨码开关设定)
每个段最多站点数	32
每个网络最多站点数	126
隔离方式	光电隔离

表 4-36　LM3401 模块的物理特性

名　称		物 理 特 性
尺寸规格		75mm(L)×90mm(W)×70mm(H)
重量		<200g
功率消耗	+24V(DC)(扩展总线提供)	0mA
	+24V(DC)(外部提供)	20mA
	+5V(DC)(扩展总线提供)	120mA
工作温度		0~+55℃
存储温度		-40~+70℃
相对温度		5%~95%，不凝结

表 4-37　指示灯的状态描述

灯	灭	绿灯亮	绿灯闪烁	红灯亮
RUN	未上电或模块坏	模块工作正常	正在建立通信	—
COMM	无通信	通信状态	—	—
ERROR	无错误	—	—	通信错误

LM3401 模块的 DB9 连接器信号定义见表 4-38，通信速率与电缆长度的对应关系见表 4-39。

表 4-38　DB9 连接器信号定义

连接针号	定义	信 号 含 义	连接针号	定义	信 号 含 义
1	屏蔽	连接到连接器外壳	6	VP	+5V，90mA
2	系统保留	—	7	系统保留	—
3	B	RxD/TxD+	8	A	RxD/TxD-
4	CNTR-P	请求发送信号 RTS(TIL 电平)	9	系统保留	—
5	DGND	+5V 地			

表 4-39　通信速率与电缆长度的对应关系

通信速率/(kbit/s)	电缆长度/m	通信速率/(kbit/s)	电缆长度/m
≤93.75	<1200	1.5	<200
187.5	<1000	3~12	<100
500	<400		

LM3401 模块的端子接线图如图 4-178 所示。

LM3401 模块的端子定义与接线说明：图 4-178 中的 L+ 和 L- 分别表示外接 DC24V 电源的正端和负端。图 4-178 中的 DP+ 和 DP- 在电路板内部，分别与 DB9 连接器的 3（B）和 8（A）号连接针相连。符号“*”表示此通道不接线或无实际物理连接。8 位拨码开关用来设置从站地址，ON 表示 0、OFF 表示 1，开关状态与站地址的二进制数值对应关系如图 4-179所示。

如 Profibus-DP 从站的站地址设置为十进制数 20，则所对应的二进制数为 00010100，设置方法如图 4-180 所示。

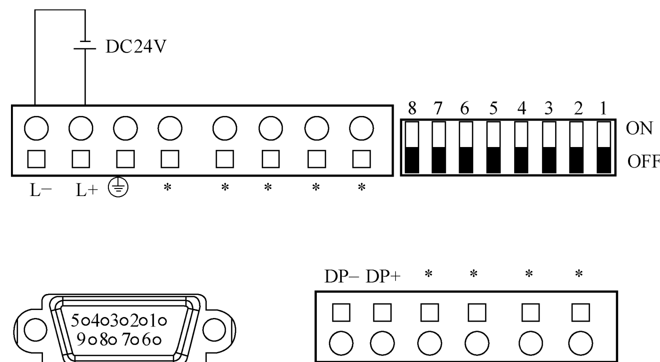


图 4-178　LM3401 模块的端子接线图

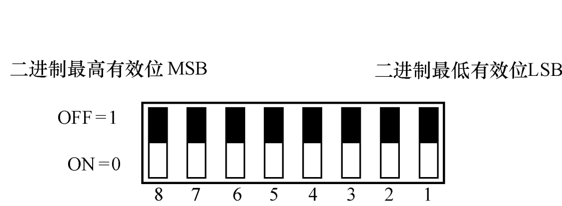


图 4-179　开关状态与站地址的二进制数值对应关系

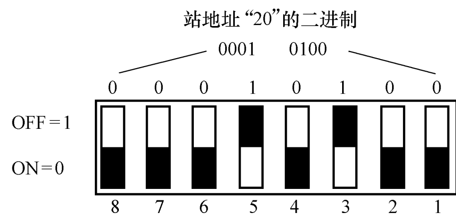


图 4-180　将从站地址设置为十进制数 20

提示：LEC G3 机可配置 Profibus-DP 模块，与 Profibus-DP 主站通信。和利时的 LK 机或西门子的 S7-300、400 机都可成为主站。和利时公司提供了配置所需要的 GSD 文件。

2. LM3401 模块软件配置

（1）把模块接入 PLC 系统

此配置在和利时编程软件的“PLC 配置”窗口上进行。如图 4-181 所示的配置是，CPU 模块用 LM3109，扩展除了输入（IAT）、输出（QAT）外，还有 LM3401Profibus-DP 从站模块。

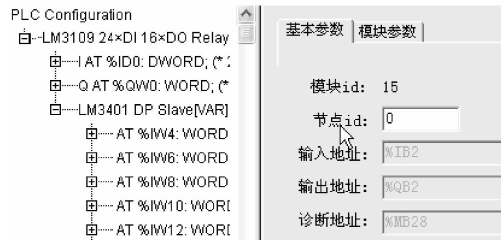


图 4-181　Profibus-DP 从站模块 LM3401 的基本参数设置

从图 4-181 可知，Profibus-DP 从站模块的节点 id 默认设置为 0（因在它之前没有别的扩展模块）。当使能此模块时，须使用这个 id 号。输入地址从% IW4 开始（因在它之前 CPU 模块占用% IW0、% IW1、% IW2、% IW3），输出地址从% QW2 开始（因在它之前 CPU 模块占用% QW0、% QW1，该图没有示出）。该网模块的模块参数设定设定如图 4-182 所示。

从图 4-182 可知，所配置 inputDataLen_Byte 为 PLC 接收数据的长度，此处设定为最大接收字节数 64。地址为% IW2 到% IW66，单号无效。outputDataLen_Byte 为 PLC 发送数据的长度，此处设定为最大发送字节数 64，地址为% QW2 到% QW64，单号无效。

（2）Profibus-DP 从站功能块使能

Profibus-DP 从站功能块 DP_Slave 包含在库文件 Hollysys_PLC_DPSlave. lib 中，用于以

Profibus-DP 从站模块使能及参数设置。其梯形图格式如图 4-183 所示，输入输出说明见表 4-40。

基本参数　模块参数

Index	Name	Value	Default	Min.	Max.
1	InputDataLen_Byte	64	0	0	64
2	OutputDataLen_Byte	64	0	0	64

图 4-182　Profibus-DP 从站模块 LM3401 的模块参数

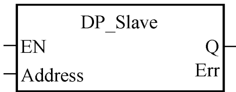


图 4-183　Profibus-DP 从站功能块 DP_ Slave

表 4-40　Profibus-DP 从站功能块 DP_ Slave 输入输出说明

通道说明	CPU 模块输入输出数据存放地址:% IWxx 和% QWxx,PLC 配置中规定的 IW 和 QW 区地址		
	参数名称	数据类型	功 能 描 述
输入	EN	BOOL	上升沿使能
	Address	BYTE	该模块节点 id:0 ~7,与 PLC 配置里的节点 id 一致
输出	Q	BOOL	是否读到有效数据,0:未读到数据;1:读到有效数据
	Err	BYTE	与从站模块通信故障号; 0:无故障; 1:等待 DP 从站模块 Ready 错; 2:读中断 DP 从站模块错; 3:读应答错; 4:读数据长度错; 5:读数据错; 6:写数据错; 7:写中断 DP 从站模块错

从说明知，设置好 id 号，调用本功能块，若通信无误，则输出字节 Err 为 0。如未读到有效数据，Q 置 1。如读到有效数据，Q 置 0。

提示：和利时 PLC 硬件模块设定基本实现了软件化。靠 PLC 运行初始程序进行相关参数。

（3） LEC G3 机 Profibus-DP 通信程序实例

本实例功能是向 Profibus-DP 主站发送 4 个字节的数据，同时从 Profibus-DP 主站接收 4 个字节的数据。

如图 4-184 所示的为其从站程序。它使用得变量声明如下：

```
VAR
    dp1: DP_Slave;
    err1: BYTE;
    pEQ: BOOL;
    useData: DWORD;
    pNE1: BOOL;
    pNE: BOOL;
    sendData: DWORD;
```

alarm：BOOL；

END_VAR

图 4-184 中节 1 为 Profibus 模块使能。节 2 先是把数据 SendData 双字传送到 Profibus-DP 从站模块的输出区% QD2，后进行“err1”与 0 比较。节 3 为当上述比较不等于 0，pEQ 的非 ON，说明通信出错，产生报警信号“alarm”。节 4 为当上述比较等于 0，pEQ ON，说明通信无误，则进行% ID4 与“useD”双字比较。如两者不等，则 pNE ON。节 5 为数据读取，把% ID4 传送给“useD”双字。其条件是：通信无误、读到有效数据及与先前读的数据不同。至于它与 Profibus-DP 主站间的数据交换则是网络自动完成的。

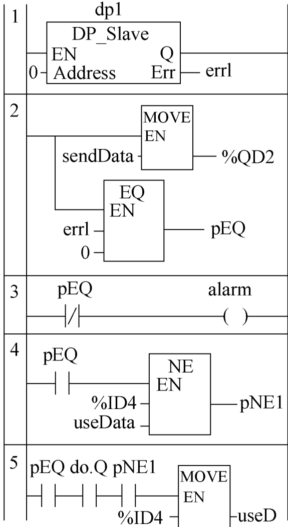


图 4-184　Profibus 从站程序

这里，对输入数据做了检查与控制。通信无误，并读到有效数据，且与先前的数据不同，才进行数据读取。对输出数据不做控制，其控制应在主站方的程序中实现。

提示：和利时 PLC 只定义有限的内部器件，但提供有客任意使用的内存。使用它之前，可按需先声明。用多少，声明多少，很灵活。

4.5.4　其他 PLC 公司 Profibus 组件

1. 三菱公司 Profibus 组件

三菱公司提供有 Profibus 网络的主站模块、从站模块。还提供 GX Develover DP 组态软件。可用其自主组建 Profibus 网络，也可与其他公司相关组件共享的 Profibus 网络。

（1）主站模块

如 QJ7IPB92D 模块。拥有以物理层，数据链接层，DDLM，以及 Profibus-DP 为基准的用户界面。使用缓冲存储器，与 PLC CPU 进行数据交换。其主要功能是：

1）可作为 Profibus-DP 的主（1 级）站。

2）通过使用输入输出信号 X/Y 以及缓冲存储器，实现主站和从站之间的输入输出数据的交换。

3）支持 9.6k、19.2k、93.75k、187.5k、500k、1.5M、3M、6M、及 12Mbit/s 的网络传输速度。可以使用配置器（Configurator）设定这些传输速率。

4）可通过使用输入输出信号 X/Y 以及缓冲存储器从从站读出故障信息。

5）通过使用全局控制功能，能够同时保持所有从站的输入输出，也可取消。

6）搭载自我检测功能，能够测试内部存储器等硬件。

7）能将输入输出数据暂存在缓冲存储器上。在处理字数据时，顺序控制程序中没有必要进行暂存。

8）在顺序控制 CPU 与 QJ71PB92D 的缓冲存储器之间进行数据传输传送时，由于使用自动刷新设定及专用命令指令，能够防止输出入输入输出数据分离。

9）在多 CPU 系统中，安装着多台 PLC CPU 模块时，可用其中任意一台 CPU 模块进行控制。

其有关规格见表 4-41 所示。

表 4-41　QJ71PB92D 模块规格

<table>
<tr><th colspan="2">项　　目</th><th colspan="3">规　　格</th></tr>
<tr><td colspan="2">机种</td><td colspan="3">QJ71PB92D</td></tr>
<tr><td colspan="2">Profibus DP 站型号</td><td colspan="3">主站(1 级)</td></tr>
<tr><td rowspan="20">传输规格</td><td>电气的标准及特性</td><td colspan="3">以 EIA-RS485 为准</td></tr>
<tr><td>媒体</td><td colspan="3">屏蔽双绞线电缆</td></tr>
<tr><td>网络构成</td><td colspan="3">总线型(但当使用中继时,为树型网络)</td></tr>
<tr><td>数据链接方式</td><td colspan="3">· 令牌冲突(主-主间)
· 轮询(主-从间)</td></tr>
<tr><td>发送符号化方法</td><td colspan="3">NRZ</td></tr>
<tr><td rowspan="10">传送速度/最大传送距离①②</td><td>传输速度/(bit/s)</td><td>传输距离[m/段]</td><td>使用 3 个中继器时的最大传输距离</td></tr>
<tr><td>9.6k</td><td rowspan="3">1200</td><td rowspan="3">4800</td></tr>
<tr><td>19.2k</td></tr>
<tr><td>93.75k</td></tr>
<tr><td>187.5k</td><td>1000</td><td>4000</td></tr>
<tr><td>500k</td><td>400</td><td>1600</td></tr>
<tr><td>1.5</td><td>200</td><td>600</td></tr>
<tr><td>3M</td><td rowspan="3">100</td><td rowspan="3">400</td></tr>
<tr><td>6M</td></tr>
<tr><td>12M</td></tr>
<tr><td>最多中继/网络数</td><td colspan="3">3 台③</td></tr>
<tr><td>最多站/段数</td><td colspan="3">32 站③</td></tr>
<tr><td>最多从站/主站数</td><td colspan="3">60 从站③</td></tr>
<tr><td>连接节数(中继数)</td><td colspan="3">32,62(1),92(2),126(3)③</td></tr>
<tr><td>可发送数据</td><td colspan="3">32 字节/1 站(通常服务模式)
244 字节/1 站(扩展服务模式)</td></tr>
<tr><td colspan="2">输入输出占有点数</td><td colspan="3">32 点(I/O 分配,智能模块 32 点)</td></tr>
<tr><td colspan="2">DC 5V 内部消耗功率/A</td><td colspan="3">0.57</td></tr>
<tr><td colspan="2">外形尺寸/mm</td><td colspan="3">105(H)×27.4(W)×97.5(D)</td></tr>
<tr><td colspan="2">重量/kg</td><td colspan="3">0.15</td></tr>
</table>

① 传输速度控制在 ±0.3% 以内（Profibus 部分 1）;
② 使用中继能够延长的传输距离（m/网络）;
传输距离（m/网络）=(中继数 +1) 传输距离（m/段）。
③ 如果存在出错信息的最大数据长度超出了 32B 的从站时，最大站，最大从站，连接节数有时会比上述值要小。

（2）从站模块

如 QJ71PB93D 模块，可与 Profibus-DP 1 级主站进行 I/O 数据通信。一个模块传送最多可达 122 字的输入或输出数据或者传送共 192 字的输入和输出数据。同时具有如下功能：

1）I/O 数据的暂存。如果 I/O 数据从主站发送或被主站所接收，则上下字节可以暂存。尽管 Profibus-DP 根据主站类型不同而采用不同方式处理 I/O 数据，但在顺控程序中 I/O 数据却不需要暂存。

2）开始/停止输入发送区域刷新。可以通过一个输出信号（Y00）控制刷新从 QJ71PB93D 向主站发送的数据。具有互锁功能，能在出现故障时防止缓冲存储数据被传送到主站。

3）扩展故障通知功能。例如，当主机出现故障时，存储于缓冲存储器故障信息扩展区

域的数据可以作为扩展故障信息传送至主站。当主机故障排除后，通知主站故障排除。

4）与全局控制功能兼容。由于与全局控制功能兼容可以通过使用 1 级主站发出的命令（SYNC，UNSYNC，FREEZE，UNFREEZE）从 1 级主站对 QJ71PB93D 的 I/O 数据进行刷新。

5）与 2 级主站进行读取输入发送区域/输出接收区域、读取 I/O 配置信息及更改站号等通信。

6）在 CPU 模块与 QJ71PB93D 缓冲存储器之间进行数据传输，为了防止 I/O 数据被分开，可采用专用指令。

7）即使多个 CPU 模块被安装在“多 CPU 系统”中，该模块仍然可以通过其中任一 CPU 模块进行控制。

等等。其有关规格见表 4-42 所示。

表 4-42　QJ7IPB93D 模块规格

<table>
<tr><th colspan="2">条　　目</th><th colspan="3">说　　明</th></tr>
<tr><td colspan="2">型号</td><td colspan="3">QJ71PB93D</td></tr>
<tr><td colspan="2">Profibus DP 站类型</td><td colspan="3">从站(符合 BN50170 卷 2(第 1、2、3、4、8 部分))</td></tr>
<tr><td colspan="2">可以设定的站号</td><td colspan="3">0 ~ 125③</td></tr>
<tr><td colspan="2">通信数据的最大传输链</td><td colspan="3">I/O 数据总共为 192 个字(输入或输出数据最多为 122 个字)</td></tr>
<tr><td rowspan="19">传输说明</td><td>电气标准和特性</td><td colspan="3">符合 EIA-RS485</td></tr>
<tr><td>媒介</td><td colspan="3">屏蔽双绞线(A 型)</td></tr>
<tr><td>网络配置</td><td colspan="3">总线(如果采用增幅器则为树型)</td></tr>
<tr><td>数据链接方法</td><td colspan="3">轮询检验方式</td></tr>
<tr><td>传输编码方法</td><td colspan="3">NRZ</td></tr>
<tr><td rowspan="11">传输速度/最大传输距离①②</td><td>传输速度/(bit/s)</td><td>传输距离/[m/段]</td><td>使用 3 个增幅器时的最大传输距离/[m/网络]</td></tr>
<tr><td>9.6k</td><td rowspan="4">1200</td><td rowspan="4">4800</td></tr>
<tr><td>19.2k</td></tr>
<tr><td>45.45k</td></tr>
<tr><td>93.75k</td></tr>
<tr><td>187.5k</td><td>1000</td><td>4000</td></tr>
<tr><td>500k</td><td>400</td><td>1600</td></tr>
<tr><td>1500k</td><td>200</td><td>800</td></tr>
<tr><td>3M</td><td rowspan="3">100</td><td rowspan="3">400</td></tr>
<tr><td>6M</td></tr>
<tr><td>12M</td></tr>
<tr><td>增幅器/网络的最大数量</td><td colspan="3">3 台②</td></tr>
<tr><td>站/段的最大数量</td><td colspan="3">32 站(包括增幅器)</td></tr>
<tr><td>连接节点/段的个数</td><td colspan="3">32</td></tr>
<tr><td colspan="2">终端电阻</td><td colspan="3">用户准备</td></tr>
<tr><td colspan="2">Flash ROH 写次数</td><td colspan="3">最多 10000 次</td></tr>
<tr><td colspan="2">占用 I/O 点数</td><td colspan="3">32 点(I/O 分配,智能模块,32 点)</td></tr>
<tr><td colspan="2">DC 5V 内耗电量</td><td colspan="3">0.44[A]</td></tr>
<tr><td colspan="2">外部尺寸/mm</td><td colspan="3">98(3.86)(H) ×27.4(1.08)(W) ×90(3.55)(D)</td></tr>
<tr><td colspan="2">重量/kg</td><td colspan="3">0.11</td></tr>
</table>

① 传输速度控制在 ±0.3% 范围内。

② 可能通过使用增幅器来增加传输距离（m/网络）。

传输距离（m/网络）=（增幅器数量 +1）传输距离（m/段）

③ 工厂设定到“126”。

2. OMRON 公司 Profibus 组件

OMRON 公司提供有 Profibus 网络的主站模块、从站模块。可用其自主组建 Profibus 网

络，也可与其他公司相关组件共享的 Profibus 网络。表 4-43 所示为它的 CJ 机 Profibus 主、从站模块的有关规格。

表 4-43 CJ 机 Profibus 主、从站模块有关规格

功　　能	CJ1W-PRM21	CJ1W-PRT21
主要功能	基础主 Profibus-DP1 级 功能插件： Set_Prm Slave_Diag Chk_Cfg Global_Control DPV1 data types support	从 Profibus 对于 DPM1 + DPM2 主站： Data_Exchange Slave_Diag Set_Prm Chk_Cfg Global_Control (SYNC/FREEZE/CLEAR) 仅对 DPM2 主站： RD_Inp RD_Outp Get_Cfg
可用网络标准	IEC 61 158/EN 50 170, Volume 2	IEC 61 158/EN 50 170, Volume 2
数据交换率/(Mbit/s)	9.6 ~ 12M	9.6 ~ 12M
最大站点支持数量	125	不可用
I/O 容量	7k 字 I/O 和 25 字 CIO	180 字 I/O
Profibus 界面	9-针雌头 sub-D 连接器	9-针雌头 sub-D 连接器
设置	旋转开关;元件数量	2 个旋转开关[Profibus-DP 的节点地址(00 ~ 99)];特殊 I/O 机器数量(00 ~ 95)
尺寸/mm	90 × 65 × 31	90 × 65 × 31
国际标准	CE, cULus, Lloyds	CE, cULus, Lloyds

OMRON 还提供 CX-ConfiguratorFDT 组态软件。此软件基于 FDT/DTM 技术。FDT 是现场设备与控制系统或工程管理工具之间数据交换的一种标准化的接口规范（IEC 62453 国际标准)。通过 FDT，可访问任何部件。FDT 是一种独立于供应商的，开放的、公开的和易于使用的规范。DTM（Device Type Manager)，设备类型管理器，是一种由设备制造商开发的软件组件，包含设备相关的应用软件。与设备一起提供。它不是一种独立的工具，DTM 通常需要 FDT 框架应用来运行。在工业自动化领域，FDT 技术可以利用 DTM 提供这种可互操作性。通过 DTM，用户可以设置设备参数、通过图形化界面操作设备、并且从任意地点获取高级的诊断信息。单一的 FDT 应用框架支持 HART、Profibus，FOUNDATION Fieldbus、DeviceNet、Interbus、AS-Interface、PROFINET IO，并将支持更多总线协议。图4-185所示的为利用该软件配置 OMRON 自主的 Profibus 网络的简况。该系统主站为 C200HW-PRM21，从站为 C200HW-PRT21 等 3 个。在其上部件类型窗口还选加需要的从站点。在图右方的 C200HW-PRM21 表单上，可对 C200HW-PRM21 特性进行组态。该软件可在线扫描所连接站点，还可通过导入部件描述文件添加其他组件。

3. AB 公司 Profibus 组件

AB 公司自身没有 Profibus 组件，但有很多公司开发了这样组件，可用于使 AB PLC 也可接入 Profibus 网络。如加拿大 WOODHEAD 公司生产的 SST-PB3-CLX-RLL 模块，其上就有 Profibus 通信口，可将 ControlLogix 处理器作为 ProfibusDP 主站或从站连入 Profibus 网络。接

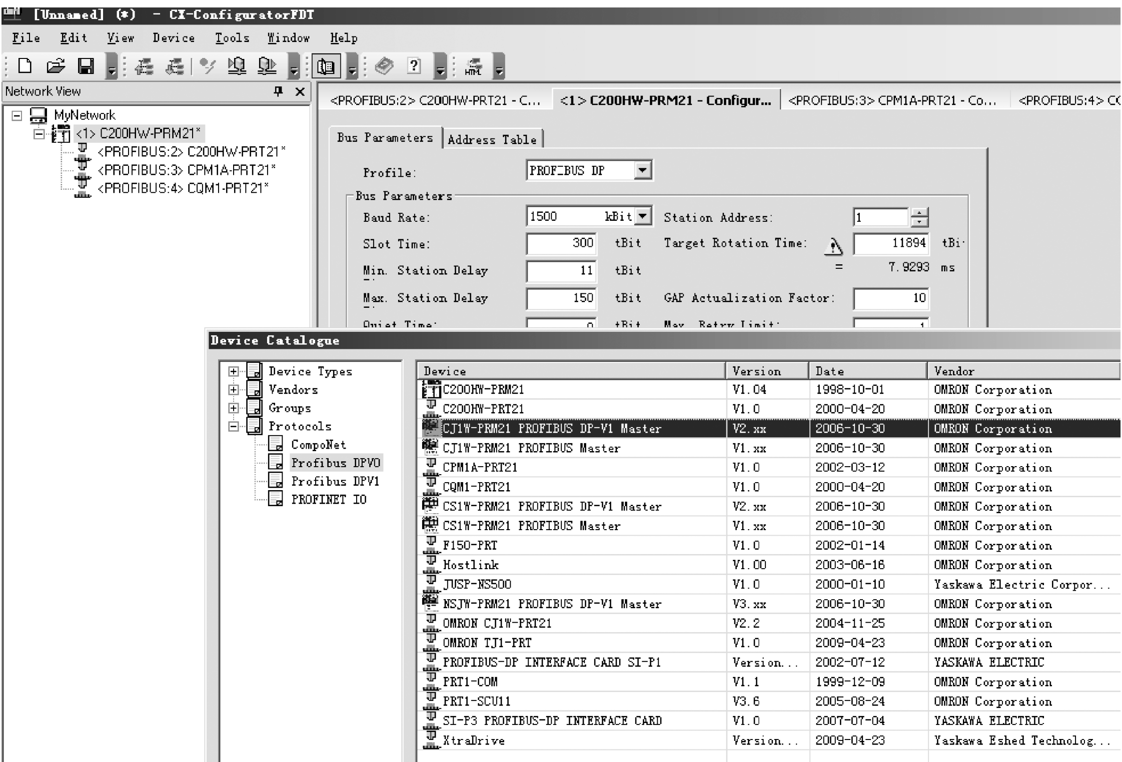


图 4-185 OMRON Profibus 网络组态简况

入后也可与其他 Profibus 相容的组件通信、交换数据。图 4-186 所示为其外观及插入 AB ControlLogix 机架的照片。



a) 外观　　b) 插入机架

图 4-186 SST PB3 外观及插入机架

SST PB3 模块是按行规交付（Add-On-Profile，AOP）的，很容易通过 RSLogix 5000 软件集成到 ControlLogix 系统中。数据从 SST 模块传送到 ControlLogix 处理器有两种方式：直接方式（Direct Mode），可多达 496 输入字节及 496 输出字节；打包方式（Pagging Mode），通过用户在 CPU 的内存定义数据区，允许访问 1984 输入字节和 1968 输出字节。

该模块使用简便，模块配置及其与处理器 ControlLogix 交换数据无须编写梯形图程序。通过 AB 的 RSLinx 可远程诊断与配置 Profibus 网络。可自动检测 Profibus 部件。在一个 ControlLogix 机架上可安装多达 8 个模块。支持当地与远程机架 ControlLogix 机架安装。等等。其网络特性见表 4-44 所示。

表 4-44 SST 模块 PB3 网络特性

协议	Profibus DP Master V0/V1, class 1&2 Profibus DP Slave V0
支持从站数	Maximum of 125
每从站 I/O	Maximum of 244 bytes in/out
自定义内存区(ControlLogix)	Maximum 1984 bytes input data Maximum 1968 bytes output data 250 words status
传输速率	All Profibus data rates up to 12Mbps
电缆	Belden 3079A Brad Hanison® 85-0001 PVR2 conductor with shield UL-listed
连接器	DB9 female connector

该模块适用于实时性要求高的远程 I/O 控制、采集远程 I/O 数据及桥接 AB 网络与其他 Profibus 网络桥接。沈阳鹭岛公司曾使用该模块组建 AB ControlLogix 架构下的 Profibus 网络。用于内蒙古大板输煤程控系统。该模块作为 Profibus 主站，而图尔克的 I/O 模块作为从站。特别适用于环境恶劣的场合。

第 5 章　PLC 信息网配置

PLC 信息网主要用于 PLC 与企业高层计算机网络互连。企业高层网络主要站点当然是计算机。这些计算机站点有的作为服务器，用以运行管理软件，存储相关数据；有的作为工作站，用以录入及使用数据。只是这些录入及使用多靠手工进行。而有了 PLC 站点接入，服务器既可直接从 PLC 得到生产一线数据，又可向 PLC 发送有关控制命令；工作站也可直接访问 PLC，使用 PLC 数据。显然，有 PLC 站点接入企业高层计算机网络，既可使 PLC 控制实现网络化、信息化，增强控制效能；又可使企业管理数据的采集、传送及使用更加及时、准确，提高企业管理效益。

本章将先简要介绍以太网发展，然后再分节介绍几个品牌 PLC 以太网的系统配置。

5.1　以太网发展

关键词：传统以太网、快速以太网、交换以太网、工业以太网

以太网（Ethernet）可以说是局域网中历史最悠久的一种。以太网的部分历史可以追溯到 1973 年。Robert Metcalfe 在他的博士论文中，描述了他对局域网技术的许多研究。毕业之后，他加入了施乐（Xerox）公司，并参与了一个小组的工作，为解决网络中零散的和偶然的堵塞继续开发。这项工作最终发展成以太网。以太网是用以太命名的，以太是一种想象中的物质，许多人曾经相信以太充满整个空间，并且是光波传输的媒质。它采用带冲突检测的载波监听多路访问协议（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）总线结构。现在泛指所有采用 CSMA/CD 协议的局域网。

IEEE802.3 标准就是在最初的以太网技术基础上开发的。在此基础上，后来又有了大发展，而且还在继续向前发展。目前以太网主要有：传统以太网、快速以太网、交换以太网、工业以太网以及做为工业以太网之一的 PLC 以太网。

以太网除了系统简单、成本低廉、组建灵活、通信速度高、技术成熟且至今还在不断进步之外，还有 TCP/IP 协议簇与其配套，还可与因特网互联。因而，软硬件丰富、使用非常普遍，优点多多，已成为当今最常用的局域网。企业的信息网几乎也都采用以太网。出现了“众网归 e（以太网）” 局面。早期 PLC 信息网也较多，如今也几乎都采用以太网，也是“众网归 e”。同时，还出现工业以太网。使其可用于工业现场，并伸向控制层、现场层，有的还成为 PLC 远程 I/O 网。为工业自动化、网络化、信息化提供了很大的发展空间。

5.1.1　传统以太网

是基于 IEEE802.3 标准的以太网。最常用的有以下 4 种。

1. 10Base-5

通常称为粗缆以太网。目前由于高速交换以太网技术的广泛应用，在新建的局域网中，10Base-5 很少被采用。

2. 10Base-2

通常称为细缆以太网。10Base-2 使用 50Ω 细同轴电缆，它的建网费用比 10Base-5 低。目前 10Base-2 也已很少被使用。

3. 10Base-T

是使用无屏蔽双绞线来连接的以太网，使用 2 对 3 类以上无屏蔽双绞线，一对用于发送信号，另一对用于接收信号。为了改善信号的传输特性和信道的抗干扰能力，每一对线必须绞在一起。双绞线以太网系统具有技术简单、价格低廉、可靠性高、易实现综合布线和易于管理、维护、升级等优点。因此比 10Base-5 和 10Base-2 技术有更大的优势，也是目前还在应用的 10M 局域网技术。

4. 10Base-F

是 10Mbit/s 光纤以太网，它使用多模光纤作为传输介质，在介质上传输的是光信号而不是电信号。因此 10Base-F 具有传输距离长、安全可靠、可避免电击等优点。由于光纤介质适宜相距较远的站点，所以 10Base-F 常用于建筑物之间的连接，它能够构建园区主干网。目前 10Base-F 较少被采用，代替它的是更高速率的光纤以太网。

5.1.2 快速以太网

有 IEEE802.3u 所定义的以太网，速度为 100Mbit/s，传输介质为双绞线。还有 IEEE802.3z 所定义的千兆以太网，速度为 1000Mbit/s，传输介质为光纤或双绞线。最新的为万兆以太网，速度为 10Gbit/s，传输介质为光纤，全双工无需 CSMA/CD 协议的网络。

1. 百兆以太网

1995 年 9 月，IEEE802 委员会正式批准了 IEEE802.3u 标准。百兆以太网就是基于 IEEE802.3u 标准的以太网，用 100M 波特率代替 10M 波特率。

（1）百兆以太网的协议结构

在 LLC 子层使用 IEEE802.2 标准，在 MAC 子层仍使用 CSMA/CD 方法，只是在物理层作了调整，并将 MAC 子层和物理层分开。定义了百兆介质专用接口（MII，Media Independent Interface）及新的物理层标准（100BASE-T）。这样，物理层在实现 100Mbit/s 速率时所使用的传输介质和信号编码方式的变化不会影响 MAC 子层。100BASE-T 目前有 3 种传输介质的标准：100BASE-TX、100BASE-T4、100BASE-FX。100Mbit/s 以太网的协议结构如图 5-1 所示。

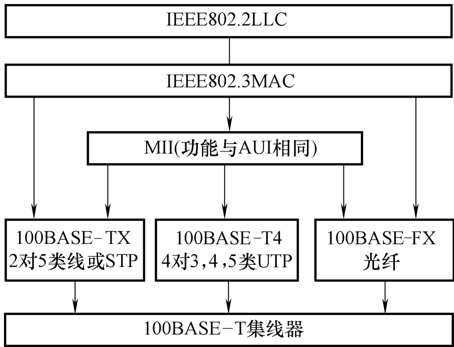


图 5-1　100Mbit/s 以太网的协议结构

（2）百兆以太网组网方式

依传输介质不同而不同。分别介绍如下：

1）100BASE-TX。100BASE-TX 是 5 类无屏蔽双绞线方案，由 10Base-T 派生出来的。100BASE-TX 类似于 10Base-T，但它使用的是两对无屏蔽双绞线（UTP）或 150Ω 屏蔽双绞线（STP）。使用的两对双绞线中，一对用于发送数据，另一对用于接收数据。由于发送和接收都有独立的通道，所以 100BASE-TX 支持全双工操作。

100BASE-TX 的硬件系统由以下几部分组成：带内置收发器、支持 IEEE802.3u 标准的网卡，5 类无屏蔽双绞线或 150Ω 屏蔽双绞线，8 针 RJ-45 连接器，100BASE-TX 集线器（Hub）。有两类 100BASE-TX 集线器，Ⅰ类和Ⅱ类。Ⅰ类集线器在输入和输出端口上可以对线路信号重新编码，所以Ⅰ类集线器可以连接使用不同编码技术的介质系统，如 100Base-TX 和 100Base-T4。Ⅱ类集线器的端口没有这种功能，它只是简单地将输入信号转发给其他端口，所以Ⅱ类集线器只能连接使用相同编码方案的介质系统，如 100Base-TX 和 100Base-FX。

100BASE-TX 的组网规则如下：

（a）各网络站点须通过 Hub（集线器，100M）连入网络中。

（b）传输介质用 5 类无屏蔽双绞线或 150Ω 屏蔽双绞线。

（c）双绞线与网卡，或与 Hub 之间的连接，使用 8 针 RJ-45 标准连接器。

（d）网络站点与 Hub 之间的最大距离为 100m。

（e）在一个冲突域中只能连接一个Ⅰ类 HUB，网络的最大直径（站点—Hub—站点）为 200m。如果使用Ⅱ类 Hub，最多可以级连两个Ⅱ类 Hub，网络的最大直径（站点—Hub—Hub—站点）为 205m。

2）100BASE-FX。100BASE-FX 是光纤介质快速以太网标准，采用与 100BASE-TX 相同的数据链路层和物理层标准协议。它支持全双工通信方式，传输速率可达 200Mbit/s。

100BASE-FX 的硬件系统包括单模或多模光纤及其介质连接部件、集线器、网卡等部件。用多模光纤时，当站点与站点不经 Hub 而直接连接，且工作在半双工方式时，两点之间的最大传输距离仅有 412m；当站点与 Hub 连接，且工作在全双工方式时，站点与 Hub 之间的最大传输距离为 2km。若使用单模光纤作为媒体，在全双工的情况下，最大传输距离可达 10km。

3）100BASE-T4。100BASE-T4 是 3 类无屏蔽双绞线方案，该方案使用 4 对 3 类（或 4 类、5 类）无屏蔽双绞线介质。它能够在 3 类 UTP 线上提供 100Mbit/s 的传输速率。双绞线段的最大长度为 100m。目前这种技术没有得到广泛的应用。100BASE-T4 的硬件系统与组网规则与 100BASE-TX 相同。

2. 千兆以太网

1998 年 2 月，IEEE802 委员会正式批准了 IEEE802.3z 标准。千兆以太网就是基于 IEEE802.3z 标准的以太网。数据传输率达到 1000Mbit/s。

（1）千兆以太网的体系结构

在 LLC 子层使用 IEEE802.2 标准，在 MAC 子层使用 CSMA/CD 方法。只是在物理层作了的调整，并将 MAC 子层与物理层分开。它定义了定义了千兆介质专用接口（GigabitMedia Independent Interface，GMII）及新的物理层标准（1000BASE-T）。这样，物理层在实现 1000Mbit/s 速率时所使用的传输介质和信号编码方式的变化不会影响 MAC 子层。千兆以太网定义了 3 种传输介质，其中两种是光纤，包括 1000Base-SX 和 1000Base-LX；另一种是铜线，分别为 1000Base-CX 及 1000BASE-T。

（2）千兆以太网的组网方式

针对 3 种介质分述如下：

1）1000Base-SX 是一种在收发器上使用短波激光作为信号源的媒体技术。这种收发器

上配置了激光波长为 770～860nm（一般为 800nm）的光纤激光传输器，不支持单模光纤，仅支持 62.5μm 和 50μm 两种多模光纤。对于 62.5μm 多模光纤，全双工模式下最大传输距离为 275m。对于 50μm 多模光纤，全双工模式下最大传输距离为 550m。1000Base-SX 标准规定连接光缆所使用的连接器是 SC 标准光纤连接器。

2）1000Base-LX 是一种在收发器上使用长波激光作为信号源的媒体技术。这种收发器上配置了激光波长为 1270～1355nm（一般为 1300nm）的光纤激光传输器。它可以驱动多模光纤和单模光纤。使用的光纤规格为 62.5μm 和 50μm 的多模光纤，9μm 的单模光纤。对于多模光纤，在全双工模式下，最长的传输距离为 550m；对于单模光纤，在全双工模式下，最长的传输距离可达 5km。连接光缆所使用的是 SC 标准光纤连接器。

3）1000Base-CX 是使用铜缆的两种千兆以太网技术之一。1000Base-CX 的媒体是一种短距离屏蔽铜缆，最长距离达 25m，这种屏蔽电缆是一种特殊规格高质量的 TW 型带屏蔽的铜缆。连接这种电缆的端口上配置 9 针的 D 型连接器。1000Base-CX 的短距离铜缆适用于交换机间的短距离连接，特别适用于千兆主干交换机与主服务器的短距离连接。

IEEE802.3 委员会公布的第二个铜线标准 IEEE802.3ab，即 1000BASE-T 物理层标准。1000BASE-T 是使用 5 类无屏蔽双绞线的千兆以太网标准。1000BASE-T 标准使用 4 对 5 类无屏蔽双绞线，其最长传输距离为 100m，网络直径可达 200m。因此，1000BASE-T 能与 10BASE-T、100BASE-T 完全兼容，它们都使用 5 类 UTP 介质，从中心设备到站点的最大距离都是 100m，这使得千兆以太网应用于桌面系统成为现实。

3. 万兆以太网

万兆以太网是一种数据传输速率高达 10Gbit/s、通信距离可延伸 40km 的以太网。万兆以太网继续使用 IEEE802.3 以太网协议，以及 IEEE802.3 的帧格式和帧大小。但由于万兆以太网是一种只适用于全双工通信方式，并且只能使用光纤介质的技术，所以它不需使用带冲突检测的载波监听多路访问协议 CSMA/CD。

（1）万兆以太网体系结构

10Gbit/s 以太网的 OSI 和 IEEE802 层次结构仍与传统以太网相同，即 OSI 层次结构包括了数据链路层的一部分和物理层的全部，IEEE802 层次结构包括 MAC 子层和物理层，但各层所具有的功能与传统以太网相比差别较大，特别是物理层更具有明显的特点。

1）三类物理层结构。在体系结构中定义了 10GBase-X、10GBase-R 和 10GBase-W 三种类型的物理层结构。

（a）10Gbase-X 是一种与使用光缆的 1000BaseX 相对应的物理层结构，在 PCS 子层中使用 8B/10B 编码，为了保证获得 10Gbit/s 数据传输率，利用稀疏波分复用技术（CWDM）在 1300nm 波长附近每隔约 25nm 间隔配置了 4 个激光发送器，形成 4 个发送器/接收器对。为了保证每个发送器/接收器对的数据流速度为 2.5Gbit/s，每个发送器/接收器对必须在 3.125Gbit/s 下工作。

（b）10GBase-R 是在 PCS 子层中使用 64B/66B 编码的物理层结构，为了获得 10Gbit/s 数据传输率，其时钟速率必须配置在 10.3Gbit/s。

（c）10GBase-W 是一种工作在广域网方式下的物理层结构，在 PCS 子层中采用了 64B/66B 编码，定义的广域网方式为 SONETOC-192，因此其数据流的传输率必须与 OC—192 兼容，即为 9.686Gbit/s，则其时钟速率为 9.953Gbit/s。

2）物理层各个子层的功能。物理层各个子层及功能如下所述。

（a）物理媒体。10Gbit/s 以太网的物理媒体包括多模光纤 MMF 和单模光纤 SMF 两类，MMF 又分 50μm 和 62.5μm 两种。由 PMD 子层通过媒体相关接口 MDI 连接光纤。

（b）物理媒体相关（PMD）子层。其主要的功能一方面是向（从）物理媒体上发送（接收）信号。在 PMD 子层中包括了多种激光波长的 PMD 发送源设备。PMD 子层另一个主要功能是把上层 PMA 所提供的代码位符号转换成适合光纤媒体上传输的信号或反之。

（c）物理媒体连接（PMA）子层。PMA 子层的主要功能是提供与上层之间的串行化服务接口以及接收来自下层 PMD 的代码位信号，并从代码位信号中分离出时钟同步信号；在发送时，PMA 把上层形成的相应的编码与同步时钟信号融合后，形成媒体上所传输的代码位符号送至下层 PMD。

（d）广域网接口（WIS）子层。WIS 子层是处在 PCS 和 PMA 之间的可选子层，它可以把以太网数据流适配 ANSI 所定义的 SONETSTS-192c 或 ITU 所定义的 SDHVC-4-64c 传输格式的以太网数据流。该数据流所反映的广域网数据可以直接映射到传输层。

（e）物理编码（PCS）子层。PCS 子层处在上层 RS 和下层 PMA 之间，PCS 和上层的接口通过 10Gbit/s 媒体无关接口 XGMII 连接，与下层连接通过 PMA 服务接口。PCS 的主要功能是把正常定义的以太网 MAC 代码信号转换成相应的编码和物理层的代码信号。

（f）协调（RS）子层和 10Gbit/s 媒体无关接口（XGMII）。RS 和 XGMII 实现了 MAC 子层与 PHY 层之间的逻辑连接，即 MAC 子层可以连接到不同类型的 PHY 层（10GBase-X、10GBase-R 和 10Gbase-W）上。显然，对于 10GBase-W 类型来说，RS 子层的功能要求是最复杂的。

（2）万兆以太网的技术特点

万兆以太网与传统的以太网比较具有以下几方面的特点。

1）MAC 子层和物理层实现 10Gbit/s 传输速率。

2）MAC 子层的帧格式不变，并保留 IEEE802.3 标准最小和最大帧长度。

3）不支持共享型，只支持全双工，即只可能实现全双工交换型 10Gbit/s 以太网，因此 10Gbit/s 以太网媒体的传输距离不会受到传统以太网 CSMA/CD 机理制约，而仅仅取决于媒体上信号传输的有效性。

4）支持星型局域网拓扑结构，采用点到点连接和结构化布线技术。

5）在物理层上分别定义了局域网和广域网两种系列，并定义了适应局域网和广域网的数据传输机制。

6）不能使用双绞线，只支持多模和单模光纤，并提供连接距离的物理层技术规范。

（3）万兆以太网在局域网中的应用

10Gbit/s 以太网用做局域网，通常是组成主干网。例如，利用 10Gbit/s 以太网实现交换机到交换机、交换机到服务器以及城域网和广域网的连接。10Gbit/s 以太网在局域网中的应用如图 5-2 所示。图中主干线路使用 10Gbit/s 以太网，校园 A、校园 B、数据中心和服务器群之间用 10Gbit/s 以太网交换机的模块分别连接。

5.1.3 交换以太网

早期的以太网，不仅速度低，而且是共享以太网（Shared Ethernet）。多站点共享同一个

传输媒体。发送站点的数据以广播的方式传输后，由每一台设备通过验证数据包头的地址确定是否接收。共享式以太网的典型代表是使用 10Base2、10Base5 的总线型网络和以集线器，也就是常说的 Hub，为核心的 10Base-T 星型网络。在使用集线器的以太网中，集线器将很多以太网设备（如计算机）集中到一台中心设备上，这些设备都连接到集线器中的同一物理总线结构中。从本质上讲，以集线器为核心的以太网同原先的总线型以太网无根本区别，同时也只能传输一个数据帧。这意味着集线器所有端口都要共享同一带宽。

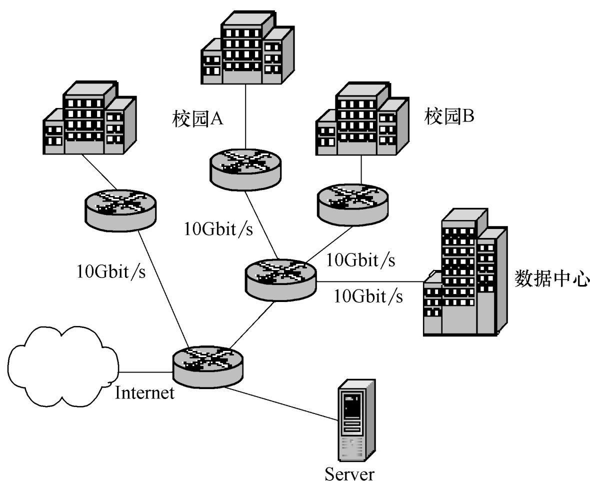


图 5-2　10Gbit/s 以太局域网应用

由于共享式以太网所有的节点都接在同一冲突域中，不管一个帧从哪里来或到哪里去，所有的节点都能接收到这个帧。随着节点的增加容易发生冲突。为避免冲突使用了 CSMA/CD技术，即发送方检测到冲突就暂停发送，随机延迟一段时间后再重新发送直到成功。由于延迟时间是随机的，不能事先知道，因而共享以太网的时间响应具有不确定性，不能用于强实时性场合。大量的冲突将导致网络性能急剧下降。

为克服了这些缺点，以太网在提高传输速度的同时，还发展交换技术，出现了交换以太网（Switched　Ethernet）。交换是按照通信两端传输信息的需要，利用交换机代替集线器。交换机拥有一条很高带宽的背部总线和内部交换矩阵，所有端口都挂接在这条背部总线上。所以，它可根据收到的数据帧中的 MAC（Media Access Control）地址，决定数据帧应发向交换机的哪个端口。因为端口间的帧传输彼此屏蔽，因此节点就不担心自己发送的帧在通过交换机时是否会与其他节点发送的帧产生冲突。使用了这种把需要传输的信息送到符合要求的对象上技术的以太网也称交换以太网。

具体讲交换机转发数据帧的规则是：如果数据帧的目的 MAC 地址是广播地址或者组播地址，则向交换机（除源端口外）所有端口转发；如果数据帧的目的 MAC 地址是单播地址，但是这个地址并不在交换机的地址表内，那么也会向交换机（除源端口外）所有端口转发；如果数据帧的目的 MAC 地址在交换机的地址表内，那么根据地址表转发到相应的端口；如果数据帧的目的 MAC 地址与数据帧的源地址在同一个端口上，它就会丢弃这个数据帧，交换也不会发生。同时，交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。可知，一般讲，交换以太网足可减少共享以太网的“冲突”，使以太网也具有确定性与实时性。

以下就交换方式、交换机类型及利用交换技术建立虚拟网络做进一步说明。

1. 交换方式

目前交换机在传送源和目的端口的数据包时通常采用直通式交换、存储转发式和碎片

隔离方式 3 种数据包交换方式。目前的存储转发式是交换机的主流交换方式。

（1）直通交换方式（Cut-through）

采用直通交换方式的以太网交换机可以理解为在各端口间是纵横交叉的线路矩阵电话交换机。它在输入端口检测到一个数据包时，检查该包的包头，获取包的目的地址，启动内部的动态查找表转换成相应的输出端口，在输入与输出交叉处接通，把数据包直通到相应的端口，实现交换功能。由于它只检查数据包的包头（通常只检查 14 个字节），不需要存储，所以其切入方式具有延迟小，交换速度快的优点。所谓延迟（Latency）是指数据包进入一个网络设备到离开该设备所花的时间。

它的缺点主要有 3 个：一是因为数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，不能提供错误检测能力；二是由于没有缓存，不能将具有不同速率的输入/输出端口直接接通，而且容易丢包。如果要连到高速网络上，如提供快速以太网（100BASE－T）连接，就不能简单地将输入/输出端口“接通”，因为输入/输出端口间有速度上的差异，必须提供缓存；三是当以太网交换机的端口增加时，交换矩阵变得越来越复杂，实现起来就越困难。

（2）存储转发方式（Store-and-Forward）

以太网交换机的控制器先将输入端口到来的数据包缓存起来，先检查数据包是否正确，并过滤掉包错误。确定包正确后，取出目的地址，通过查找表找到想要发送的输出端口地址，然后将该包发送出去。正因如此，存储转发方式数据处理延时大，但是它可以对进入交换机的数据包进行错误检测，并且能支持不同速度的输入/输出端口间的交换，可有效地改善网络性能。它的另一优点就是这种交换方式支持不同速度端口间的转换，保持高速端口和低速端口间协同工作。实现的办法是将 10Mbit/s 低速包存储起来，再通过 100Mbit/s 速率转发到端口上。

（3）碎片隔离式（Fragment Free）

这是介于直通式和存储转发式之间的一种解决方案。它在转发前先检查数据包的长度是否够 64B（512 bit），如果小于 64B，说明是假包（或称残帧），则丢弃该包；如果大于 64B，则发送该包。该方式的数据处理速度比存储转发方式快，但比直通式慢，但由于能够避免残帧的转发，所以被广泛应用于低档交换机中。

使用这类交换技术的交换机一般是使用了一种特殊的缓存。这种缓存是一种先进先出的 FIFO（First In First Out），比特从一端进入然后再以同样的顺序从另一端出来。当帧被接收时，它被保存在 FIFO 中。如果帧以小于 512bit 的长度结束，那么 FIFO 中的内容（残帧）就会被丢弃。因此，不存在普通直通转发交换机存在的残帧转发问题，是一个非常好的解决方案。数据包在转发之前将被缓存保存下来，从而确保碰撞碎片不通过网络传播，能够在很大程度上提高网络传输效率。

2. 交换机类型

交换机类型很多，如果根据工作协议层划分，有：第二层交换机、第三层交换机和第四层交换机。这是随着交换技术的发展而发展的。

1）第二层交换机是对应于 OSI/RM 的第二协议层来定义的，因为它只能工作在 OSI/RM 开放体系模型的第二层，即数据链路层。第二层交换机依赖于链路层中的信息（如 MAC 地址）完成不同端口数据间的线速交换，主要功能包括物理编址、错误校验、帧序列

以及数据流控制。这是最原始的交换技术产品，目前桌面型交换机一般是属于这类型，因为桌面型的交换机一般来说所承担的工作复杂性不是很强，又处于网络的最基层，所以也就只需要提供最基本的数据链接功能即可。第二层交换机应用最为普遍（主要是价格便宜，功能符合中、小企业实际应用需求），一般应用于小型企业或中型以上企业网络的桌面层次。

2）第三层同样是对应于 OSI/RM 开放体系模型的第三层，即网络层来定义的，也就是说这类交换机可以工作在网络层，它比第二层交换机更加高档，功能更加强。第三层交换机因为工作于 OSI/RM 模型的网络层，所以它具有路由功能，它是将 IP 地址信息提供给网络路径选择，并实现不同网段间数据的线速交换。当网络规模较大时，可以根据特殊应用需求划分为小面独立的 VLAN 虚拟网段，以减小广播所造成的影响时。通常这类交换机是采用模块化结构，以适应灵活配置的需要。在大中型网络中，第三层交换机已经成为基本配置设备。

3）第四层交换机是采用第四层交换技术而开发出来的交换机产品，当然它工作于 OSI/RM 模型的第四层，即传输层，直接面对具体应用。第四层交换机支持的协议是各种各样的，如 HTTP、FTP、Telnet、SSL 等。在第四层交换中为每个供搜寻使用的服务器组设立虚 IP 地址（VIP），每组服务器支持某种应用。在域名服务器（DNS）中存储的每个应用服务器地址是 VIP，而不是真实的服务器地址。当某用户申请应用时，一个带有目标服务器组的 VIP 连接请求（例如一个 TCPSYN 包）发给服务器交换机。服务器交换机在组中选取最好的服务器，将终端地址中的 VIP 用实际服务器的 IP 取代，并将连接请求传给服务器。这样，同一区间所有的包由服务器交换机进行映射，在用户和同一服务器间进行传输。

第四层交换技术相对原来的第二层、第三层交换技术具有明显的优点，从操作方面来看，第四层交换是稳固的，因为它将包控制在从源端到宿端的区间中。另一方面，路由器或第三层交换，只针对单一的包进行处理，不清楚上一个包从哪来、也不知道下一个包的情况。它们只是检测包报头中的 TCP 端口数字，根据应用建立优先级队列，路由器根据链路和网络可用的站点决定包的路由；而第四层交换机则是在可用的服务器和性能基础上先确定区间。

有了这么多类型的交换机，完全可根据确定性及实时性的要求选用，以组建合乎要求的交换以太网。

3. 基于交换机应用的虚拟局域网

虚拟局域网技术（VLAN，英文 Virtual Local Area Network 的缩写）是交换技术的发展，主要是基于交换机（只有三层以上交换机才具有此功能）和路由器的应用。有了它，可根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域。每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。VLAN 除了能将网络划分为多个广播域，从而有效地控制广播风暴的发生，以及使网络的拓扑结构变得非常灵活的优点外，还可以用于控制网络中不同部门、不同站点之间的互相访问。

VLAN 在交换机上的实现方法很多，如基于端口的、基于 MAC 地址的、基于 IP 地址的及按用户定义的，等等。

目前最常用的是基于端口的实现。这种实现是将交换机上的物理端口和内部的 PVC（永久虚电路）端口分成若干个组，每个组构成一个虚拟网，相当于一个独立的 VLAN 交换机。这种实现的优点是定义 VLAN 成员时非常简单，只要将所有的端口都定义为相应的 VLAN 组即可。它的缺点是如果某用户离开了原来的端口，到了一个新的交换机的某个端口，必须重新定义。

基于 MAC 地址的是，交换机对站点的 MAC 地址和交换机端口进行跟踪，在新站点入网时根据需要将其划归至某一个虚拟局域网，而无论该站点在网络中怎样移动，由于其 MAC 地址保持不变，因此用户不需要进行网络地址的重新配置。基于 IP 地址的是，交换机根据各站点网络地址自动将其划分成不同的虚拟局域网。新站点在入网时无需进行太多配置。

4. 以太网 IP 地址及子网划分

在此，顺便介绍以下 IP 地址及子网掩码的有关问题。

（1）IP 地址（Internet Protocol Address）

是分配给每个站点的 32 位各不相同的数字，以作为各个站点在网络上相互区分的标识。显然，各个站点所设定的 IP 地址应该是唯一的，否则无法相互识别。

IP 地址的 32 位二进制数分成 4 段，每段 8 位，中间用小数点隔开，然后将每八位二进制数转换成十进制数。而实际上，每个 IP 地址是由网络号和站点号两部分组成。前者用来标识该网络在 Internet 上的网络号（Network ID），后者用来标识该站点在该网络上的站点（Host ID 号。网际地址分解成两个域后，带来了一个重要的优点是，IP 数据包从网际上的一个网络到达另一个网络时，选择路径可以基于网络而不是主机。在大型的网际中，这一点优势特别明显，因为路由表中只存储网络信息而不是主机信息，这样可以大大简化路由表。

根据网络上的站点多少，网络可分为：大型、中型及小型 3 种。分别对应于有 A 类、B 类、C 类 3 种 IP 地址。此外考虑其他用途，还有 D、E 类地址以及不用于公网而专用于私（局部）网的 IP 地址。

1）A 类 IP 地址。由 1 字节的网络地址和 3 字节主机地址组成。二进制网络地址的首位规定为 0。此外，IP 地址全为 0 也另有应用。所以它的网络号只能在 1 ~ 126 之间选定。而它每个网络的主机则可在 0 ~ 2 的 24 次方之间选定。可容纳 1 亿多个主机。

2）B 类 IP 地址。第一和第二段号码为网络号，剩下的 2 段号码为计算机的号。二进制网络地址的最高 2 位规定是“10”。所以，它的第一段网络号可在 128 ~ 191 之间选定。加上第 2 段地址可在 0 ~ 255 之间选定，所以，它可用的网络有 16382 个。而它每个网络的主机可在 1 ~ 2 的 16 次方之间选定。可容纳 6 万多个主机。

3）C 类 IP 地址。第一、第二、第三段号码为网络号，剩下的最后一段号码为计算机号。二进制网络地址的最高 3 位必须是“110”。所以，它的第一段网络号可在 192 ~ 223 之间选定。加上第 2、3 段地址，所以，它可用的网络可达 209 万余个，每个网络能容纳 254 个主机。

4）D 类 IP 地址。第一个字节二进制数以“1110”开始，地址范围为 224 ~ 239，是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

5）E 类 IP 地址。第一个字节二进制数以“11110”开始，为将来使用保留。

6）特殊 IP 地址。有 2 个特殊 IP 地址。全零（“0.0.0.0”）对应于当前主机。全“1”

当前子网的广播地址。

7）私网 IP 地址。国际规定有一部分 IP 地址不在公网中使用，只用于局域网（私网）。其范围是：

10. 0. 0. 0 ~ 10. 255. 255. 255

172. 16. 0. 0 ~ 172. 31. 255. 255

192. 168. 0. 0 ~ 192. 168. 255. 255

在日常网络环境中，基本是都在使用 B、C 两大类地址，而 A、D、E 这 3 类地址都不大可能用到。

（2）子网及子网掩码

有了上述 IP 地址，怎么识别它所在的网络及它在网络中的地址呢？可使用网络掩码。掩码也是一个 32 位数。通过与 IP 地址逻辑运算，屏蔽或获取 IP 地址的一部分数值，进而区别网络号和主机号。如上述 C 类网络，其掩码可以用 255. 255. 255. 0。将其与 IP 地址进行与运算，所得出的值就是此 IP 地址所处的网络号。如要读取它的主机号，则可先把此掩码取反，然后再与 IP 地址进行与运算，所得出的值就是该 IP 地址在网络上的主机号。

如果把这个工作延伸，利用不同的掩码还可把以上各类网络划分较小的网络，即所谓子网。以一个 C 类的 IP 地址段 192. 168. 0. 1 ~ 192. 168. 0. 254 为例，这里 192. 168. 0 是这个网络号，而 1 ~ 254 表示这个网段中的主机号。它最大能容纳 254 个主机。如果不用上述 255. 255. 255. 0 掩码，而用 255. 255. 255. 128 掩码，则这个 C 类地址可区分为 2 个网络，一个容纳的主机为 192. 168. 0. 1 ~ 192. 168. 0. 127。另一个容纳的主机为 192. 168. 0. 128 ~ 192. 168. 0. 255。在每个网络中最多只能容纳 128 台主机。再如还是上述 C 类地址，假如子网掩码 255. 255. 255. 192（也就 8 主机位，被占用了 2 位，二进制表示为 11111111. 11111111. 11111111. 11000000），那么这个网段的电脑主机数目就是 $2^6=64$ 台，总共有 $2^2=4$ 个网段。第一个网段为 192. 168. 0. 1 ~ 192. 168. 0. 63，第二个网段为 192. 168. 0. 64 ~ 192. 168. 0. 127，第三个网 段为 192. 168. 0. 127 ~ 192. 168. 0. 191，第四个网段为 192. 168. 0. 192 ~ 192. 168. 0. 254。

其他类地址划分子网的方法也类似。总是舍弃掉主机若干个二进制的首地址位用以编码，可划分相应的子网。如舍弃 1 个首位，则划分 2 个子网。2 个首位，则 4 个子网。N 个首位数，则 2^N 个子网。而主机数业相应减少。如 C 类地址舍弃 N 个首位，则只有 2^{8-N}个主机数目。

正是有这样的子网划分，所以，以太网的各个站点除了要设置 IP 地址，还要设置子网掩码。这样，各站点可对其地址与子网掩码进行逻辑运算，得出是否与对方处于同一子网。同处一个子网，则可直接通信。否则就要通过路由器实现通信。

提示：虚拟网与子网是不同的。虚拟局域网从硬件上隔离广播，能有效减少网络中的广播流量。子网是用子网掩码划分，并不隔离广播，不能减少网络流量。通常一个 VLAN 应该对应一个子网。如果两个站点同处一个虚拟网而不在同一子网中，或反过来，要通信就要借助路由器。

5. 1. 4　工业以太网

工业以太网似乎没有严格的定义，但通俗地讲，就是用于工业环境的以太网，是以太网

或者说是互联网系列技术延伸到工业应用的产物。以太网技术原本不是为工业应用准备的，但改进其环境适应性及通信确定性、实时性，并添加了一些应用功能后，才逐步发展与形成这个工业以太网的。

1. 工业以太网特点

（1）环境适应性

产品要适应工业控制现场的恶劣环境。具体包括机械环境适应性（如耐振动、耐冲击)、气候环境适应性（工作温度要求为 -40 ~ +85℃，至少为 -20 ~ +700℃，并要耐腐蚀、防尘、防水)、电磁环境适应性或电磁兼容性 EMC 应符合 EN 50081-2、EN 50082-2 标准。在易爆或可燃的场合，工业以太网产品还需要具有防爆要求，包括隔爆、本质安全两种方式。

（2）工作可靠性

工业以太网工作要可靠。必要时可冗余配置。目前冗余工业以太网，其最大网络重构时间可短到 0.3s。

（3）信息安全性

如果运用互联网技术，还有个网络安全问题。要防安全隐患，如病毒、工业间谍、黑客、软件 BUG、恐怖主义等。

（4）安装方便性

要适应工业环境的安装要求。为如一些公司专门开发和生产了导轨式收发器、集线器和交换机系列产品，安装在标准 DIN 导轨上，并有冗余电源供电，接插件采用牢固的 DB9 结构等。另外，一些公司还专门开发和生产了用于工业控制现场的加固型连接件（如加固的 RJ45 接头、具有加固 RJ45 接头的工业以太网交换机、加固型光纤转换器/中继器等)，可以用于工业以太网变送器、执行机构等。有的还可提供向站点供电，如 24VDC，以便使无电源供应的站点也能正常工作。

（5）通信实时性、确定性

实时性是指系统在定义的时间内能处理完外部事件。确定性是指系统以一种可预见的（确定性）方式进行响应。工业以太网如果用于传递信息，确定性、实时性要求相对不高。但如果用于控制要求就高了。为此，世界各大公司都有相应对策，如使用交换以太网以至于用全双工以太网、或也采用令牌传输机制等。

当然，不是所有工业以太网都具有以上这些特点。具体取决于它的使用环境及应用目的。表 5-1 所示为工业以太网设备与商用以太网设备的主要区别。

表 5-1 工业以太网设备与商用以太网设备大体区别

	工业以太网设备	商用以太网设备
元器件	工业级	商用级
接插件	耐腐蚀、防尘、防水，如加固型 RJ45、DB-9、航空接头等	一般 RJ45
工作电压	DC 24V	AC 220V
电源冗余	双电源	一般没有
安装方式	可采用 DIN 导轨或其他方式固定安装	桌面、机架等
工作温度	-40 ~ 85℃或 -20 ~ +70℃	5 ~ 40℃

（续）

	工业以太网设备	商用以太网设备
电磁兼容性标准	EN 50081-2（工业级 EMC） EN 50082-2（工业级 EMC）	EN 50081-2（办公室用 EMC） EN 50082-2（办公室用 EMC）
MTBF 值	至少 10 年	3～5 年

2. 工业以太网类型

工业以太网类型与其具体应用有关，不同的应用就有不同的工业以太网。如果从与以太网标准的关系及确定性、实时性来看，大体有：标准工业以太网及基于以太网；特高确定性、实时性工业以太网、高确定性、实时性工业以太网及一般工业以太网。

（1）标准工业以太网及基于以太网

标准工业以太网就是，无论从实施标准还是实现功能它都与以太网完全兼容。与普通以太网不同的只是考虑工业的需要，增加一些通信协议、功能及选件。标准工业以太网的好处是，可方便采用以太网产品，可分享以太网的进步技术。这也是目前开发工业以太网的主流。

基于以太网则是部分使用以太网标准或在以太网标准的基础上做些修改，在功能上除了与普通以太网兼容外，也增加了与工业控制有关的应用。基于以太网更能体现工业的特点，但在网络组建上，可能会有所不便，而且当以太网又有了新进步，可能还要做相应再开发，才能分享它的成果。

（2）确定性、实时性工业以太网

工业以太网可以不具备确定性、实时性。早期的 PLC 以太网多是如此。其功能就是能与企业的计算机网络互联，以至于接入互联网，能实现 PLC 与企业网络数据交换，也可接收、发送邮件。此外，有的工业以太网的站点也具有 WEB 功能，计算机也可通过使用浏览器对其访问，上传或下载数据。但这些工作的确定性、实时性要求都不高。延时 100ms，以至更多都是可以接受的。早期的工业以太网也多是此类应用。

特高、高确定性、实时性工业以太网主要用于工业控制。确定性、实时性的保证有两种方法：一是使用高速与交换以太网，确保减少或避免以太网常见的介质访问冲突；二是在高传输速率的基础上，其介质访问控制也采用令牌技术，靠令牌有序的传输确定站点的数据发送权，以避免介质访问冲突，确保通信的确定性、实时性。目前，高确定性、实时性工业以太网实时性可确保在 10ms 左右，特高确定性、实时性工业以太网实时性可确保在 1ms 左右。前者多用于现场总线，后者则用于运动控制及时间同步控制。

5.1.5　PLC 以太网

PLC 以太网是工业以太网重要组成。PLC 厂家在推出控制网的同时，几乎也都推出自身的以太网。目的是使自身 PLC 能廉价与方便地与企业信息网互连，实现 PLC 与计算机非实时的数据交换。而这个工作往往还有更廉价与方便的串口网络也可完成，只是串口网络速率低些就是了。再就是，由于这个以太网的功能有限，确定性、实时性还没有解决，也没有组建协会性支持组织，所以实际采用的还不是很多。但进入 21 世纪以来，由于以太网及现场总线技术的进步，PLC 以太网发展也很快，功能也有所增加，已得到广泛的应用。并组建了多个国际性协议组织，形成了几个各有其特点的开放的 PLC 以太网。如 EtherNet/IP、Modb-

us TCP/IP 、PROFInet 及 CC-Link IE 等。本章除了介绍一些公司专用的 PLC 以太网之外，还将介绍上述这些开放 PLC 以太网。

5.2 和利时 PLC 以太网配置

关键词：IP 地址、网关地址、子网掩码、Modbus TCP/IP

和利时产 LM 机拥有 LM3403 以太网模块，也可接入以太网。它的以太网与 MODBUS TCP 协议兼容。可用以使 LM 机作为 ModbusTCP 以太网从站，以实现与以太网中 Modbus TCP 以太网主站通信。Modbus TCP/IP 是法国施耐德公司开发的，是目前工业以太网的标准之一。

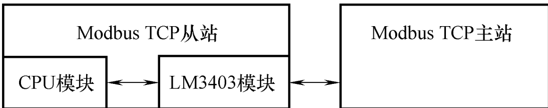


图 5-3 LM3403 模块的网络功能图

图 5-3 所示为它的连网简图。

5.2.1 LM 机以太网模块特性

LM3403 模块物理特性见表 5-2 所示。其 RJ45 接口用于连接以太网线，指示灯的状态描述见表 5-3 所示。LM3403 模块的特性见表 5-4 所示。

表 5-2 LM3403 模块物理特性

名　称		物理特性
尺寸规格		75mm(*L*) ×90mm(*W*) ×70mm(*H*)
重量		<200g
功率消耗	+24VDC(扩展总线提供)	0mA
	+24VDC(外部提供)	0mA
	+5VDC(扩展总线提供)	80mA
工作温度		0℃ ~ +55℃
存储温度		-40℃ ~ +70℃
相对湿度		5% ~95%,不凝结

表 5-3 指示灯的状态描述

灯(状态)	灭	绿灯亮	绿灯闪烁	红灯亮
RUN	未上电或模块坏	模块工作正常	—	—
LINK	以太网连接未建立	以太网连接建立	—	—
RX/TX	没有数据收发	—	数据收发	—
ERROR	无错误	—	—	通信错误

表 5-4 LM3403 模块通信功能

名　称	功能描述
通信口数量	1 个通信口,同一时间只能和一个 Modbus TCP 主站通信
接口类型	RJ45
协议类型	Modbus TCP 从站

（续）

名　　称	功 能 描 述
配置所需内容	IP 地址、子网掩码、网关 IP、读写数据长度， IP 地址的出厂默认值为 172.20.45.160，MAC_Address 不需配置
通信速率	100Mbit/s
输入输出区大小	最大各 200B
每个网络最多站点数	取决于组态软件

5.2.2　LM 机以太网模块功能

LM 机以太网模块用于使 LM 机接入以太网。但只能作为一个 ModbusTCP 从站，接受 ModbusTCP 主站发送的命令，并按要求予以自动处理与回应。本身无法主动发起通信。

LM 机用到 Modbus TCP 的功能见表 5-5 所示。

表 5-5　ModbusTCP 的功能描述

功　能　码	名　　称	作用（对主站而言）
01	读取开出状态	取得一组开关量输出的当前状态
02	读取开入状态	取得一组开关量输入的当前状态
03	读取模出状态	取得一组模拟量输出的当前状态
04	读取模入状态	取得一组模拟量输入的当前状态
05	强制单路开出	强制设定某个开关量输出的值
06	强制单路模出	强制设定某个模拟量输出的值
15	强制多路开出	强制设定多个开关量输出的值
16	强制多路模出	强制设定多个模拟量输出的值

ModbusTCP 协议和 ModbusRTU 协议的区别在于：

第一，它没有从站地址这个概念，它寻址所依靠的是 IP 地址。

第二，在它的命令帧及数据帧中，没有 CRC 校验码。但是在帧之前要加入一些字节。字节的具体内容见表 5-6 所示。

表 5-6　Modbus TCP/IP 协议格式参考表

字节	说　　明
0	站点 ID 一般为 0
1	站点 ID 一般为 0
2	协议 ID＝0 为 0
3	协议 ID＝0 为 0
4	从字节 6 到帧尾（数据帧）的字节数（高位）＝0（因为帧长度应该小于 256 个字节，因此，此位为 0）
5	从字节 6 到帧尾（数据帧）的字节数（低位）
6	地址识别，这一字节一般只是在 Modbus 桥接的时候用，在目前 LM3403 的接法，没有作用，一般为 0，模块不对这一位做判断
7	Modbus 功能码，诸如 0×05
8	后面就开始 Modbus 数据和地址，这个和 ModbusRTU 一致，只是不用校验

第三，它只能从图 11-25 中表示的输出区读数据。也只能对图 11-25 表示的输入区写数据。具体地址可以在其中选择。

例：要用 05 功能码写 LM3403 的第一个位（%IX4.0），其命令格式见表 5-7 所示。

表 5-7　写位数据命令格式举例

站点 ID		协议 ID		6~11:6 个字节		地址识别	功能码	起始地址		置位状态	原状态
0	1	2	3	4	5	6	7	8	9	10	11
00	00	00	00	00	06	00	05	00	00	FF	00

表 5-8 表示的为和利时 LM3403 以太网模块寄存器区与 Modbus TCP 功能码对照参考表。

表 5-8　以太网模块寄存器区与 Modbus TCP 功能码对照表

区	读写	功能码		Modbus 地址与寄存器地址对应关系举例	
I	只写	位	0×05	%IX4.0	0
				%IX4.1	1
				%IX6.1	17
		字	0×06	%IW4	0
				%IW6	1
				%IW8	2
Q	只读	位	0×02	%QX 和%QW 与 I 区的对应关系相同	
		字	0×04		

注：1. 这里的 I 和 Q 区是 LM3403 设定的寄存器区。

2. 在进行网络通信时，PLC 编程软件通过串口可以同时连接 PLC，以监视和设置 PLC 各寄存器的状态和数值。

3. 位地址计算：如果位的地址为%IXx.y，那么，命令中的地址为（x－z）＊8＋y。如字的地址为%IWm，那么，命令中的地址为（m－z）/2。这里的 z 为%IW 区开始地址。%QW 区计算方法与此类似。本表计算 I 地址，假设 z 为 4。计算 Q 地址，假设 z 为 2。

5.2.3　LM 机以太网设置

首先，要在要在 PLC 配置窗口上设置。然后，还要在程序中使能。才能完成入网配置。

1. 在 PLC 配置窗口上设置

利用和利时编程软件，打开 PLC 配置窗口如图 5-4 所示，的 PLC 配置窗口，配置的 CPU 模块是 LM3109，扩展为 LM3403 以太网模块。

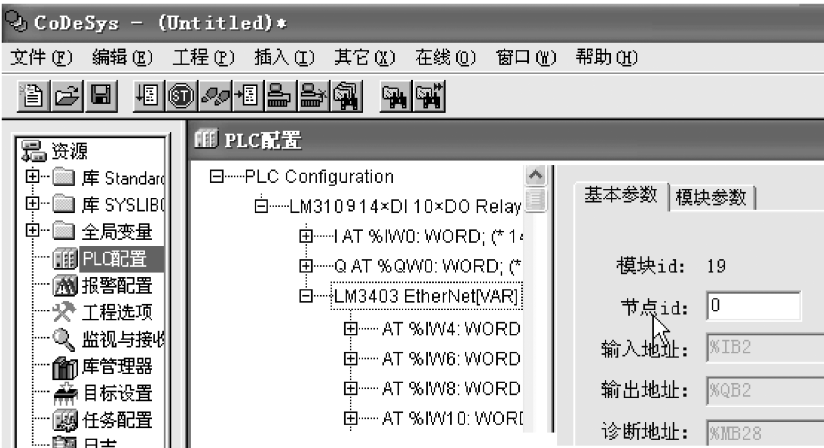


图 5-4　以太网模块 LM3403 的基本参数配置

从图可知，以太网模块的站点 id 默认设置为 0（因在它之前没有别的扩展模块）。当使能此模块时，须使用这个 id 号。输入地址从% IW4 开始（因在它之前 CPU 模块占用% IW0、% IW1、% IW2、% IW3），输出地址从% QW2 开始（因在它之前 CPU 模块占用% QW0、% QW1，该图没有示出）。以太网模块的 IP 地址、子网掩码、网关、输入输出区大小等通信参数设定如图 5-5 所示。



图 5-5　以太网模块 LM3403 的模块参数

PLC 以太网都是 C 类。所设定的 IP 地址不能与其他通信站点相同，否则无法通信。

子网掩码必须与计算机的子网掩码一致。图 5-4 设的 IP 地址为 169. 254. 202. 1，子网掩码为“255. 255. 255. 0”。IP 地址与掩码“与”运算后得出的 169. 254. 202 是网络号，而 1 是站点号。这个网络号必须与通信对方的网络号相同。

网关地址也必须与通信对方的网关地址一致。图 5-4 设的为“169. 254. 202. 168”。而 MAC_ Address 可不填。

ReadDataLen_ Byte 为 PLC 接收数据的长度，此处设定为最大接收字节数 200。地址为% IW4 到% IW202，单号无效。WriteDataLen_ Byte 为 PLC 发送数据的长度，此处设定为最大发送字节数 200。地址为% QW2 ~ % QW200，单号无效。

2. 以太网模块使能程序设置

（1） EtherNet_ TCP 以太网功能块

EtherNet_ TCP 以太网功能块包含在库文件 Hollysys_ PLC_ EtherNet. lib 中，用于以太网模块使能及参数设置。其梯形图格式如图 5-6 所示，输入输出说明见表 5-9。



图 5-6　以太网功能块 EtherNet_ TCP

表 5-9　以太网功能块 EtherNet_ TCP 输入输出说明

通道说明	CPU 模块输入输出数据存放地址：% IWxx 和% QWxx，PLC 配置中规定的 IW 和 QW 区地址		
	参数名称	数据类型	功能描述
输入	EN	BOOL	上升沿使能
	Address	BYTE	读模块站点 id：0-7，与 PLC 配置里的站点 id 一致
输出	Q	BOOL	是否读到有效数据，0：未读到数据；1：读到有效数据
	Err	BYTE	与以太网模块通信的故障号 0：无故障 1：等待以太网模块 Ready 错 2：读中断以太网模块错 3：读应答错 4：读数据长度错 5：读数据错 6：写数据错 7：写中断以太网模块错

（2）EtherNet_ TCP 以太网模块使能程序

如图 5-7 所示的为以太网模块使能程序。以下为它使用的变量声明：

```
VAR
    EtherNet_TCP1:EtherNet_TCP;        (＊定义功能块＊)
    err1:BYTE;                         (＊以太网通信的故障号＊)
    di1:BOOL;                          (＊定义布尔型变量＊)
    do1:BOOL;                          (＊定义布尔型变量＊)
    END_VAR
```

从图 5-7 可知，它的地址就是图 5-4 设置的 id 号 0。当 di1 置位时，功能块使能，调用以太网模块。如果设置数据有效，do1 置位。当 di1 复位时，不调用以太网模块，do1 复位。

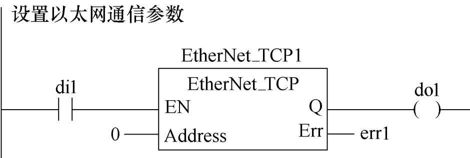


图 5-7　以太网模块使能程序

5.2.4　LM 机以太网使用实例

本例用于污水处理厂控制。在 3 个现场控制站是用 PLC 实施控制。3 个 PLC 与中央控制室之间，构筑了基于光纤工业以太网的通信网络。网络通信协议为 TCP/IP。通信介质为四芯多模光纤。若 PLC 站发生故障，该 PLC 站负责监控的设备仍可以通过切换开关实现手动控制。在中央控制室内，用两台监控计算机监控全厂设备的运行。监控计算机同时作为 I/O 服务器，其上运行和利时公司的监控软件，服务器做冗余配置，实现双机热备。只要需要分布在厂内其他位置的计算机也可以方便地通过局域网与服务器相连。

现场控制级接受生产管理级的调度，但并不依赖于生产管理级而运行。若监控计算机出现故障或者并没有投入使用或者通信网络出现故障，各现场控制站仍继续正常工作，对整个工艺过程没有影响。

在每个现场控制站安装有用于监控的触摸屏，在现场就可以直观地查看本工艺段的运行情况，画面切换按钮能够方便地切换至其他任何一幅画面。通过授予权限，操作人员也可以在现场输入工艺参数或启停设备。已安装的现场设备一般都配备就地控制箱，以实现设备的就地手动控制。就地手动控制具有最高的优先级，主要应用在设备调试和维护阶段。

该方案成功应用于五湖治理的重点工程——忻州污水处理项目，取得良好的效果，并实现了“现场无人值守，总站少人值班”的目的。

5.3　AB PLC 以太网配置

关键词：EtherNet/IP、CIP、标准以太网、隐式信息通信（Implicit）、显示信息通信（Explicit）

AB 公司以太网使用 Ethernet/IP 协议。以下先对 Ethernet/IP 做简要介绍。然后再对 AB 的以太网产品及其配置实例做具体说明。

5.3.1　Ethernet/IP 简介

Ethernet/IP 工业协议是 ODVA 开发的一个开放的工业网络标准。它支持实时 I/O 数据交换，显式信息传送，或两者兼有。它是开放的标准网络。

1. Ethernet/IP 以太网组成

典型的 Ethernet/IP 以太网组成如图 5-8 所示。

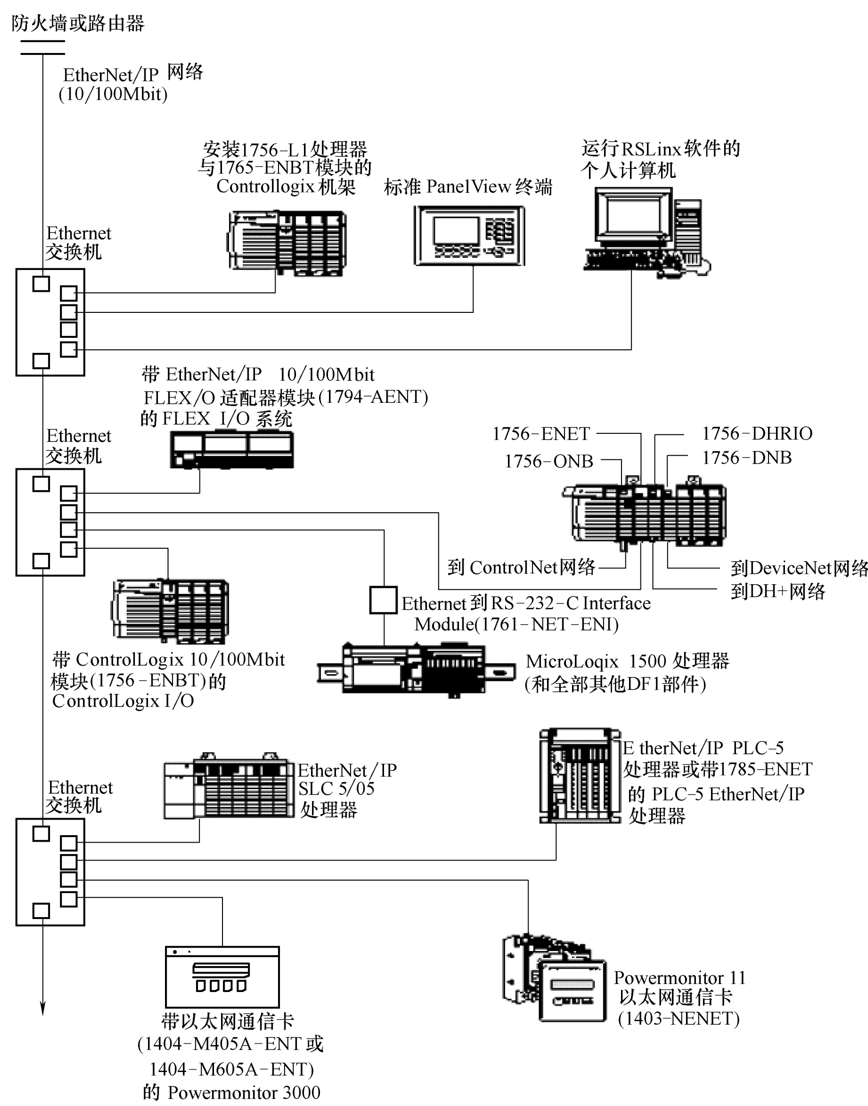


图 5-8　典型的 Ethernet/IP 以太网组成

从图知，它上有防火墙及路由器，既可接因特网，又可已防止黑客入侵。之下为 EtherNet/IP 网。图示有 3 个交换机，相互用双绞线连接。同时每交换机也是用双绞线连接若个站点。这些站点除了计算机、人机界面外，都是 AB 的、配置有以太网模块或接口 PLC 控制器、I/O 机架或 I/O 部件及运动控制器。可以看出，它的组成除了 PLC 控制器、I/O 部件及

运动控制器是 AB 专有的，其他都是以太网通用产品，系统并不复杂。

2. Ethernet/IP 网络模型

图 5-9 所示为 Ethernet/IP 的网络模型。

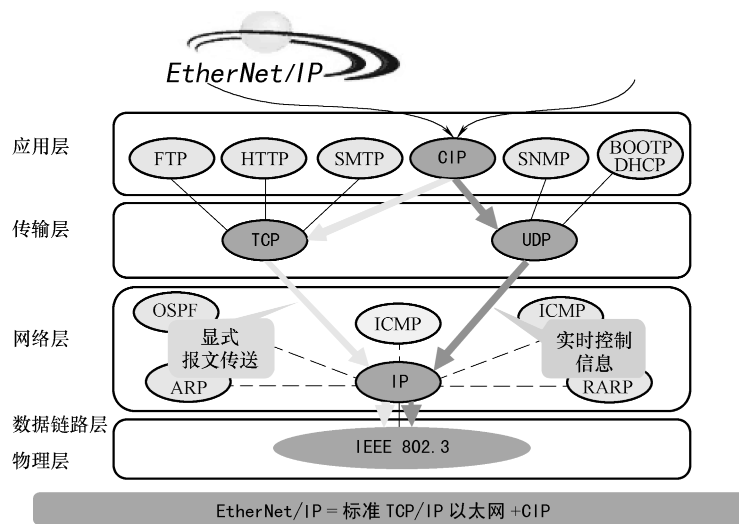


图 5-9 Ethernet/IP 网络模型

从图知，它有 4 层：底层、网络层、传输层及应用层。底层为物理层及数据链路层，遵循 IEEE802.3 标准的以太网协议。网络层、传输层使用标准的 TCP/IP 协议。应用层除了使用标准的互联网种种协议外，还与 CompoNet、DeviceNet 及 ControlNet 一样，使用合乎 ODVA 标准的通用工业协议 CIP。可知，实际上，EtherNet/IP = 标准 TCP/IP 以太网 + CIP。

3. 网络拓扑结构

EtherNet/IP 网络的拓扑使用的是星形结构。一组站点通过交换机进行点对点连接。而交换机间也是一对一连接。这样结构好处是，由于交换机具有速度自动协商功能，故可支持 10M、100M 产品，以及它们混合使用。同时还易于接线与维修。

除了使用交换机，如果实时性要求不高，也可使用价格较低的集线器。为了与其他网络相连，也可接路由器。为了网络安全，也可加防火墙。

使用的传输介质，除了双绞线还可使用光缆及相应转换器。为增加传输距离，也可使用中继器。由于目前以太网已广为应用，相关产品是很多的，这就为对其配置提供了很多选择。

4. 通信类型

EtherNet/IP 的 CIP 的控制部分用于实时 I/O 数据交换或称隐式信息通信（Implicit）。CIP 的信息部分用于显示信息通信（Explicit）。表 5-10 所示为与这个定义对应的 EtherNet/IP 通信类型。

表 5-10 Ethernet/IP 通信类型

Ethernet/IP 传送类型	信息类型	说　明	举　例
信息	显示	无时间限制数据	通过信息指令读/写数据
I/O 数据	隐式	实时 I/O 数据	远程 I/O 部件实时控制数据
实时互锁	隐式	实时部件互锁	两处理器间实时交换数据

信息数据。没有严格时间要求的数据传输，典型的如大数据包数据。信息数据使用源站点与目标站点之间生命期短的显式连接。信息数据包使用 TCP/IP 协议，并利用 TCP 的数据处理特性。

I/O 数据。实时性要求苛刻的数据交换。典型的如相对小的数据包。I/O 数据交换使用源站点与目标站点之间长期的隐式连接。I/O 数据包使用 UDP/IP 协议，并利用 UDP 高速数据处理能力。

实时互锁。在一个数据生产处理器与任意个数据消费处理器之间数据周期同步。互锁数据包使用快速的 UDP/IP 协议，并利用 UDP 高速数据处理能力。

此外，Ethernet/IP 还有 HTTP 通信类型。大部分 EtherNet/IP 模块内具备 web 服务器功能。所以可通过通用的网络浏览器，在与其联网的计算机上即可访问它。根据 EtherNet/IP 模块的具体性能，进而可对其读写数据，诊断，发送 E-mail 以及进行配置等。

5. Ethernet/IP 特点

1）用的标准的 TCP/IP 以太网，而不是基于或修改的 TCP/IP 以太网。这一点非常有意义。既为它充分利用 TCP/IP 以太网的资源及功能提供了保证，还可随着后者的发展而“与时俱进”。

2）单一网络可实现多种功能。这从它具有多种通信类型可以看得很明显。此外，还有 CIP MOTION 运动控制、CIP Sync（同步）及 CIP 安全。运动控制采集监控同步达 100 纳秒，而 CIP Sync 可实现 100ns 同步。

3）标准、成熟、可靠。整个网络架构都有公开的标准可依。而且这些标准已日趋成熟，并在实践中证明非常可靠，并得到多个标准组织支持。据称 Modbus TCP 也已加盟此标准。

4）可以在 AB NetLinx 架构内实施同一应用层 CIP 协议的 ControlNet、DeviceNet 及 CompoNet 网络实现无缝桥接和路由，为多网合一提供的可能。

5）可高效使用网络带宽。这时因为，它使用的生产者消费者模型数据可不要多次传送。以太网的网速是很高的，还有提高的趋势。其带宽有很大的可利用的空间。为此，它还可利用 TCP/IP 以太网的技术优势，开发诸如语音、图像传输，增加站点的可见性，进而充分利用网络的带宽。

6）集成各种 IT 功能的现场总线。

7）面向对象的编程与设备组态技术。

5.3.2　AB 以太网组件

1. AB 以太网组件

上述介绍 EtherNet/IP 组成中的产品，AB 公司提供的主要有适配器类、扫描器类产品。此外还有通信介质及其有关产品。

（1）EtherNet/IP 通信模块

有的用作扫描器、消息桥接器，有可用作适配器。针对 Logix5000 系列 PLC，AB 公司提供的这些模块见表 5-11 所示。

表 5-11 Logix5000 系列 PLC EtherNet/IP 通信模块

EtherNet/IP 模块	通过控制器发起通信(扫描器/网桥)	离散量 I/O 模块接口(适配器)
1756-ENBT	×	×
1756-EWEB(1)	×	
1769-L32E, -L35E	×	
1788-ENBT	×	
1794-AENT		×
1734-AENT		×

上述模块有如下特性：支持报文发送、生产者/消费者标签及远程 I/O 数据通信；可使用标准的 TCP/UDP/IP 协议封装 Ethernet/IP 信息；与 ControlNet、DeviceNet 使用共同的 CIP 协议；使用 RJ45 接口，使用 5 类无屏蔽双绞线；支持半/全双工，10M 或 100M 字适应；不需要网络规划；不需要路由表配置。可带电接入与退出网络。

（2）扫描器用的控制器产品

EtherNet/IP 通信模块与其结合后成为网络的扫描器。控制器就是各种 AB PLC 的 CPU。当今其主流产品为 Logix5000。具体见表 5-12 所示。

表 5-12 Logix5000 主流产品

特点	MicroLogix 1500	CompactLogix	FlexLogix	ControlLogix
内存(最大)	14K 字节	15M 字节	512K 字节	8M 字节
I/O(最大)	最多 256 点 由本地扩展嵌入	最多 30 Compact I/O 模块	512 点(数字量) 或 128 点(模拟量), 或者是二者的混合	128000 点(数字量) 或 3800 点(模拟量)
本地 I/O	1769Compact I/O(MicroLogix1500 唯一)	1769 Compact I/O	1794 FLEX I/O 1797 FLEX Ex I/O	1756 I/O
EtherNet/IP 网络 I/O	无	(CompactLogix 1769-L35E 唯一) 1734 POINT I/O 1756 ControlLogixI/O 1794 FLEXI/O 1797 FLEX EXI/O	1734 POINT I/O 1756 ControlLogix I/O 1794 FLEXI/O 1797 FLEX EX I/O	1734 POINT I/O 1756 ControlLogix I/O 1794 FLEX I/O 1797 FLEX EXI10
编程软件	RSLogix 500	RSLogix 5000	RSLogix 5000	RSLogix 5000
编程语言	梯形图	梯形图,FBD (功能块图),SFC(顺序 功能图),ST(结构文本)	梯形图,FBD (功能块图),SFC(顺序 功能图),ST(结构文本)	梯形图,FBD (功能块图),SFC(顺序 功能图),ST(结构文本)
接口需求	1761-NET-ENI	集成到 ControlLogix L35E 控制器,或使用 1761-NET-ENI	1788-ENBT,或使 用 1761-NET-ENI	1756-ENBT,或 使用 1761-NET-ENI

（3）适配器用的分布式模块化 I/O 产品

EtherNet/IP 通信模块与分布式模块化 I/O 及基于机架 I/O 结合将成为网络的适配器。这里基于机架 I/O 与当地使用的没有区别。分布式模块化 I/O 及其配套的适配器见表 5-13。

表 5-13　分布式模块化 I/O 及其配套的适配器

分布式模块化 I/O	选择适配器	技术指标
1734 POINT I/O	1734-AENT	· 高度模块化(可混合,与用户的精确需求匹配) · 可拆卸端子块 · 具有带电插拔(RIUP)的特点 · 易于分散 · 全范围的数字量、模拟量、专用及温度模块 · 可达 252 点/适配器
1794 FLEXI/O	1794-AENT	· 具有带电插拔(RIUP)的特点 · 24/48V 直流 · 120/230V 交流 · 继电器输出、模拟量、温度、专用、计数器及系列模块 · 4 ~ 32 点/模块
1797 FLEX EX I/O	1794-AENT(在防爆场合配用 1797-BIC 和 1797-CEC)	· 用在防爆场合的具有本征安全性的 I/O · 独立于端子块基座的模块 · 具有带电插拔(RIUP)的特点 · 数字式(NAMUR)模拟量、温度、频率 · 2 ~ 16 点/模块

此外还有其他适配器产品。如配置有以太网接口的变频器、操作员等。品种规格也很多，具体略。

(4) 其他产品

多为通用，可以按要求选购。

(5) 相关软件

有编程软件与网络软件，用以进行网络设置。

5.3.3　AB 以太网配置实例

上已提及，AB 公司的 Logix5000 系列 PLC 只有内存区。用户使用时也要根据需要定义。这个定义的形式就是 AB PLC 的标签（Tag）。

(1) 计算机接入 EtherNet/IP 及 PLC 用于远程 I/O 控制的配置

图 5-10 为其配置实例。

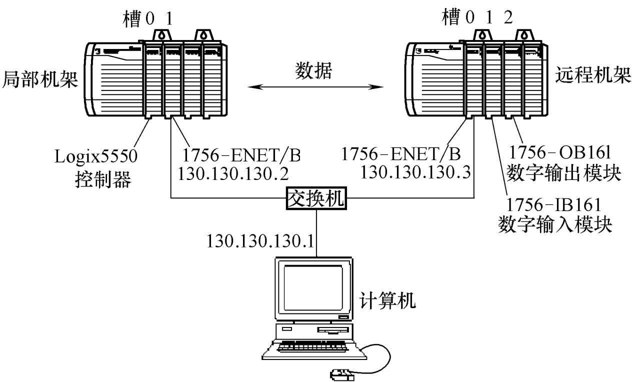


图 5-10　计算机接入 EtherNet/IP 及 PLC 用于远程 I/O 控制配置

从图知，这里有计算机以太网网卡、当地机架上的以太网通信模块及远程机架上的以太网通信模块，都是通过交换机及通信介质相互连接，以组成 EtherNet/IP 网络。在此例中，如同计算机接入 ControlNet 网络一样，也可运行 AB 相关软件，监控 PLC 及网络。此外，当地机架上的以太网通信模块作为扫描器可与作为适配器的远程机架上的以太网模块交换数据，组成 PLC 远程 I/O 网络，使当地机架上的 Logix5000 控制器与管理当地 I/O 一样管理远程 I/O。

为了配置此系统，除了安装系统、接线之外，首先要通过 RSLinx 驱动程序将计算机连接到 RSLogix 5000 项目。其次是将以太网通信模块添加到 RSLogix 5000 项目中。具体步骤与 ControlNet 网络的配置类似，可参阅本书第 4 章第 4 节 AB ControlNet 实例。图 5-11 为它的 I/O 配置结果。

从图知，本例当地及远程都有以太网模块，分别命名为 Local_ ENET 及 Remote_ ENET。并在远程机架上还添加有数字输入模块及数字输出模块，分别命名为 Remote_ Digit_ Input 及 Remote_ Digit_ Output。

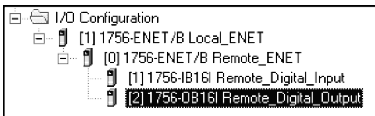
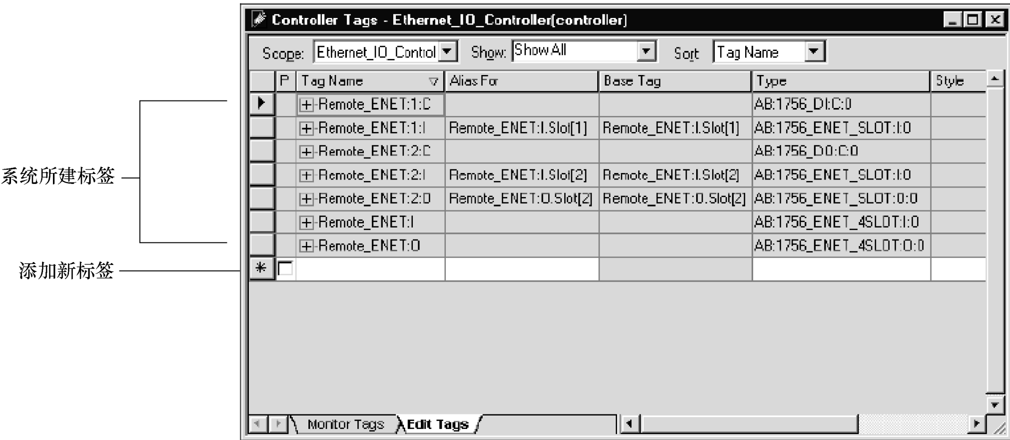


图 5-11　本例 I/O 配置

由于 I/O 标签在 I/O 模块配置后会自动生成，所以这时双击控制器标签，可观察到此标签。图 5-12 所示即为本例 I/O 标签中远程部分。



P	Tag Name	Alias For	Base Tag	Type	Style
	Remote_ENET:1:C			AB:1756_DI:C:0	
	Remote_ENET:1:I	Remote_ENET:I.Slot[1]	Remote_ENET:I.Slot[1]	AB:1756_ENET_SLOT:I:0	
	Remote_ENET:2:C			AB:1756_DO:C:0	
	Remote_ENET:2:I	Remote_ENET:I.Slot[2]	Remote_ENET:I.Slot[2]	AB:1756_ENET_SLOT:I:0	
	Remote_ENET:2:O	Remote_ENET:O.Slot[2]	Remote_ENET:O.Slot[2]	AB:1756_ENET_SLOT:O:0	
	Remote_ENET:I			AB:1756_ENET_4SLOT:I:0	
	Remote_ENET:O			AB:1756_ENET_4SLOT:O:0	

图 5-12　本例 I/O 标签

这样，对运程 I/O 的管理如同当地一样。当然随后的工作还有编程、与 PLC 联机、下载设置、下载程序等。这里不赘述。

（2）两或多个控制器联网配置

图 5-13 为其配置实例。从图知，这里有站点 1 上计算机以太网网卡、站点 2 的以太网通信模块及站点 3 上的以太网通信模块，都是通过交换机及通信介质相互连接，以组成 EtherNet/IP 网络。站点 2、3 机架上都配置有控制器，目的是通过 EtherNet/IP 实现控制器间标签链接实时数据交换。为实现控制器之间标签链接通信，还要做数据生产者/消费者设置。至于信息通信（用执行通信指令，通过非预定时段通信），以及各控制其所控制的本地与远程 I/O 这里不讨论。那是 PLC 网络编程要处理的问题，将在通信编程一书中介绍，这里略。以下将对有关标签链接的有关设置做具体说明：

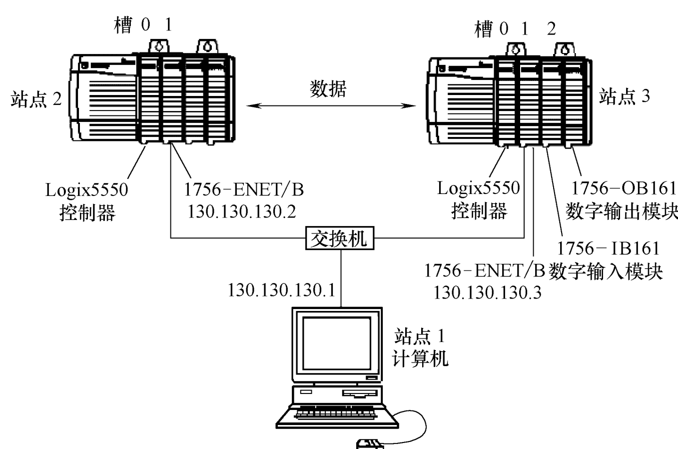


图 5-13　两个控制器联网配置

1）创建生成生产者标签的应用。其具体步骤是：

（a）创建新工程。运行 RSLogix5000 软件，打开它的一个例程。建立新工程，输入控制器名称为“Producer”，选择槽位与类型合适的机架，做好所需要的 I/O 配置，并存储文件。

（b）添加生产者标签。在如图 5-14 所示工程窗口双击“Controller Tags”项，将出现如图 5-15 所示 Controller Tags 窗口。

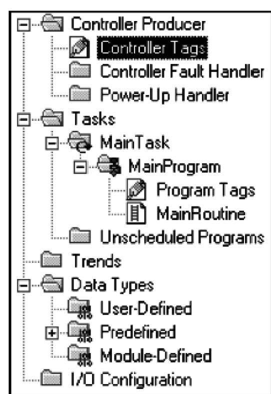


图 5-14　工程窗口



图 5-15　Controller Tags 窗口

在其上添加名称 Produced_ data 及 T1，类型分别为 DINT 及 TIMER 的两个标签，如图 5-16 所示。

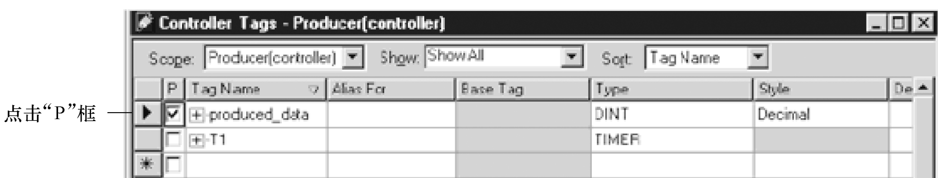


图 5-16　控制器标签窗口

这时可点击图示 P 处或用鼠标右击该标签名，在出现图 5-17 所示窗口上，点击“Edit Tag Properties”项。将弹出如图 5-18 所示标签属性窗口。

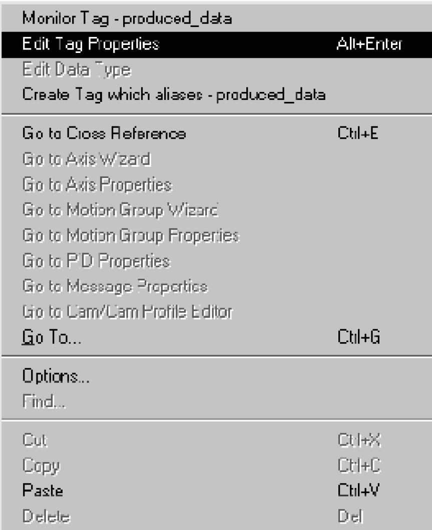


图 5-17 点击图示 P 处或用鼠标右击该标签名的窗口

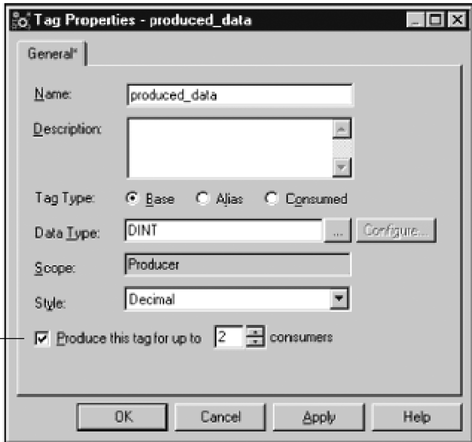


图 5-18 所示标签属性窗口

在此窗口上标签类型为生产者，并选定其消费者为两个（可在 1 ~256 之间选定）。

（c）编写程序，点击 Communications 菜单项，选定“ Who Active”，将弹出如图 5-19 所示“ Who Active”窗口，在其上将显示已安装的驱动。

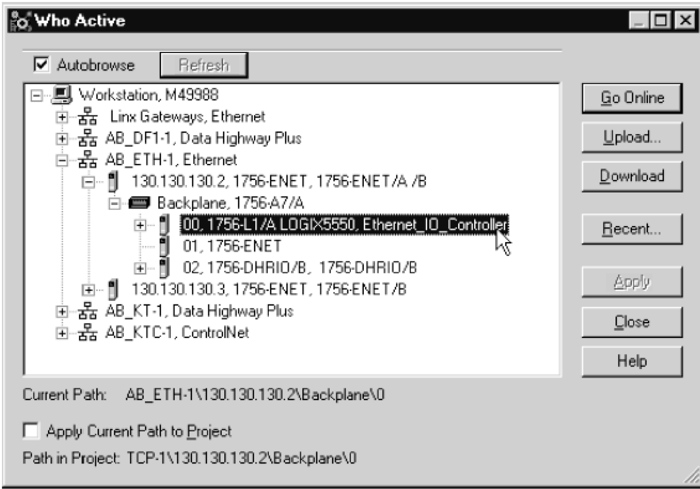


图 5-19 “ Who Active”窗口

（d）在其上选择以太网驱动（即 AB_ ETH-1），并在当地机架上的展此下拉项 。点击在“Logix 5550”及加亮的“ Download”按钮。之后，将显示如图 5-20 所示“Download”窗口。

（e）点击“Download”窗口上“Download”按钮，下载设置于程序。

（f）置 PLC 与运行模式。

（g）最小化本 RSLogix 5000 例程。

2）创建生成消费者标签的应用。目的是增加生产者标签到到此应用的 I/O 配置中，添加接收数据的消费者标签，并测试其效果。具体步骤是：

（a）运行“RSLogix5000 ”打开它的又一例程（原例程仍运行）。

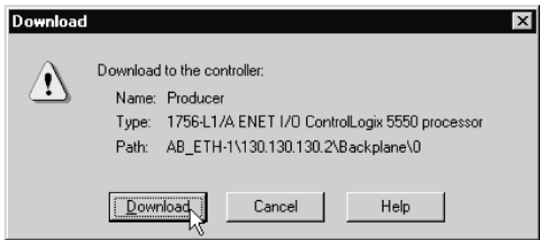


图 5-20　“Download”窗口

提示：RSLogix5000 软件可多例程，但在一个例程上创建的工程只能针对一个控制器，而不像西门子、OMRON 编程软件一个例程创建的过程可处理多个 PLC。

（b）创建新工程。运行 RSLogix5000 软件，打开它的一个例程。建立新工程，输入控制器名称为“Consumer”，选择槽位与类型合适的机架，做好所需要的 I/O 配置。

（c）添加生产者标签到本工程控制器的 I/O 配置中。为此：

a）在工程窗口中，用鼠标右肩点击“ I/O Configuration”项，将弹出如图 5-21 所示下拉菜单窗口。

b）在下拉菜单上选择新模块（New Module），将弹出如图 5-22 所示选择模块窗口。

c）选择“1756-ENET/B ”模块，并点击“OK”。之后将弹出如图 5-23 所示模块特性（Module Properties）窗口。在该窗口输入 Name、IP 地址等有关项目如图所示。

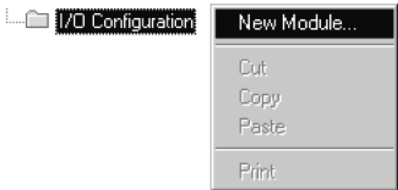


图 5-21　下拉菜单

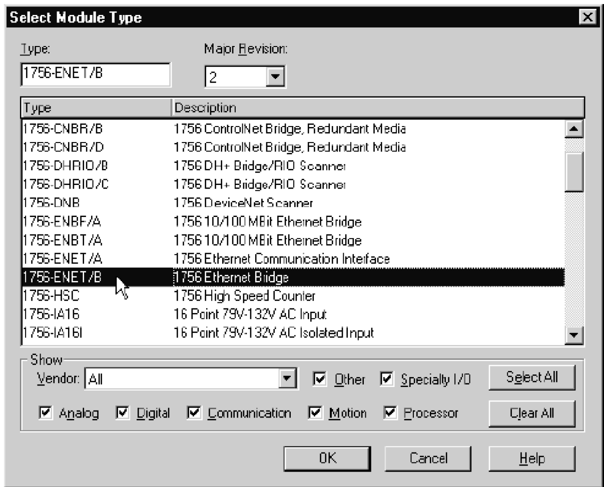


图 5-22　选择模块窗口

d）再点击“Finish”，接收此配置后，1756-ENET/B 模块将显示在它的 I/O 配置项中（如图 5-24a 所示）。进而，还必须把原当地的 1756-ENET/B 模块作为子模块添加到本应用中。做法是，用鼠标右键点击图 5-24a 的 1756-ENET/B Local_ ENET 项，然后出现如图 5-24b所示下拉菜单。

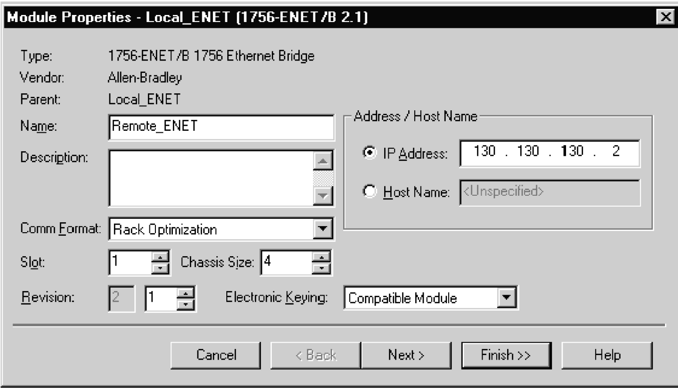


图 5-23　模块特性（Module Properties）窗口

e）从下拉菜单中选择新模块（New Module），并在随后又出现的如图 5-21 所示的选择模块类型（select Module Type）的窗口中。

f）在窗口中选择 1756-ENET/B 模块，并点击“OK”按钮。之后又弹出图 5-22 模块特性窗口。但这时选用的 IP 地址为 130. 130. 130. 2，其他一样。

g）点击“Finish ”按钮，接受这个配置。这时 I/O 在配置文件夹中，远程的 1756-ENET/B Remote_ ENET 模块 将缩进显示在当地的 1756-ENET/B Local_ ENET 之下，如图 5-25a 所示。

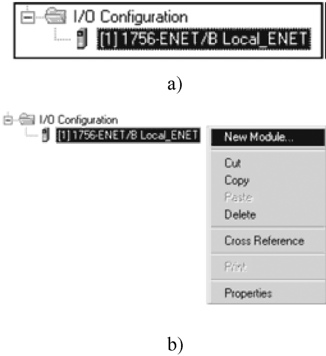


图 5-24　I/O 文件夹及下拉菜单

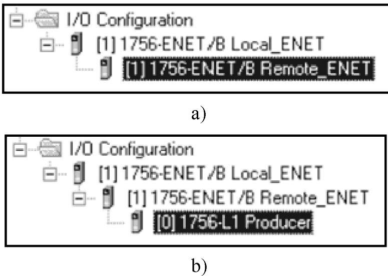


图 5-25　I/O 在配置文件夹

h）添加远程控制器（生产者）到 I/O 配置中，并置于远程 1756-ENET/B 模块之下，如图 5-25b 所示。具体过程略。

（d）通过如图 5-26 所示工程窗口创建消费者标签。其过程是：

a）用鼠标右键双击图 5-27 所示“Controller Tags”项，将又出现图 5-28 控制器标签窗口。

b）在控制器标签窗口上，添加“cunsumsed_ data”标签，如图 5-27 所示。数据类型也是 DINT。

c）与创建“produced_ data”一样，打开标签特性窗口，如图 5-28 所示。不过此时卡选定标签类型为“Consumed”。并且，在“Controller”项打开后可看到

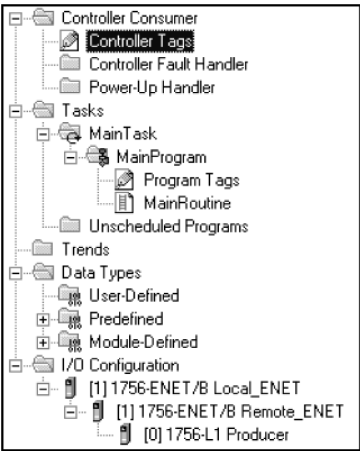


图 5-26　工程窗口

“Producer”控制器（因为它在运行，并与本控制器联网）。具体参数按表 5-14 所示选定。

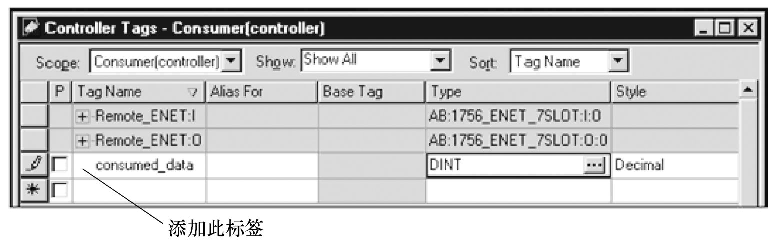


图 5-27　添加“cunsumed_ data”标签

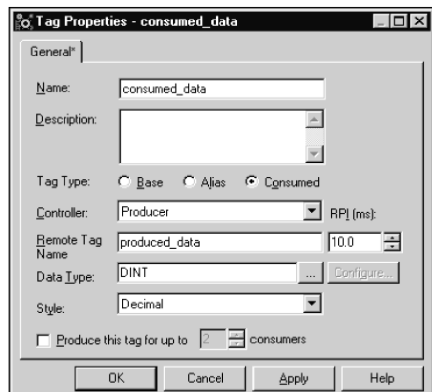


图 5-28　标签特性窗口

表 5-14　“cunsumed_ data”标签参数

名称	Comsumed_data
标签类型	消费者
控制器	生产者 *
运程标签	Produced_data
数据类型	DINT
格式	十进制
RPI	10ms

* 参数必须与生产者标签一致

d）点击“OK”按钮，存储标签特性。接着要下载这个消费应用配置给消费应用控制器，并置其处运行模式。为此，当然也与下载生产者应用一样做相应操作。具体过程略。

（e）测试。这时，如果联机生产者应用，并置“Produced_ data”一个值，如 8888，则转过来使消费者应用联机观察“consumed_ data”的值，即可看到它也将是 8888。

（f）当然还可以创建更多的消费者应用。那样的结果就是，一个数据多个使用。也可在消费者应用中创建生产者标签，在生产者应用中创建消费者标签。那样的结果就是，消费者应用向生产者应用传送数据。具体设置与上述类同，这里不再赘述。

提示：建立这样标签总数是有限制。这如同一个单一控制器所能处理的 I/O 总数有限一样。这里的限制主要来自网络的传输能力。

（3）EtherNet/IP 实现 WEB 功能配置

AB 以太网模块都可实现 WEN 功能。即使用 1756-ENET/B 这样模块，当做好系统配置，并计算机与其联网后，在计算机上运行浏览器，输入模块的 IP 地址，也可看到如图 5-29 所示的网页。

从图知，这网页提供有：Module Information（模块信息），TCP/IP Configuration（TCP/IP 配置），Diagnostic Information（诊断信息）及 Chassis Who（机架信息）项。对其中任一项点击，还可显示相应窗口，更具体的看到进一步信息。而且，如同对其他浏览器操作一样，这个点击还可层层深入，直到了解全部要了解与可了解到的信息。具体说明这里略。

此外，AB 还有 WEB 服务器增强型的以太网模块，如 1756-EWEB 和 1768-EWEB，具有更强的 WEB 服务器功能。如：模块可创建网页或“数据视”（Data Views），让远程浏览器

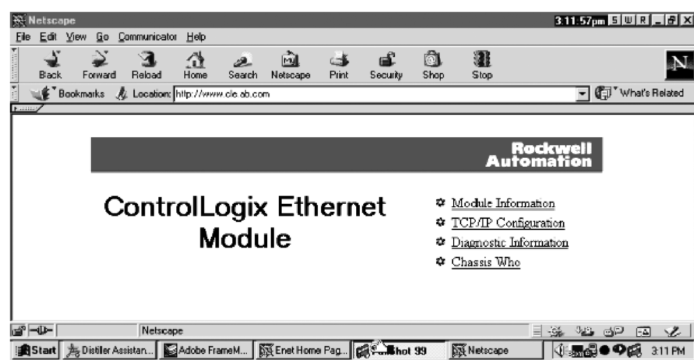


图 5-29　EtherNet/IP 网页

访问控制器实时数据；模块所在的控制器可使用信息指令，通过 Email 发传送控制系统数据和信息，更便于维修人员及时处理有关问题；模块可用 XML（可扩展标示语言）文件在数据视上存储数据，便于外部应用访问，分享系统数据；等等。

5.4　OMRON PLC 以太网配置

关键词：EIP、网络变量、标签数据链接、带宽利用率

5.4.1　以太网组件

OMRON 以太网组件主要是以太网模块或 PLC CPU 上集成的以太网接口。而以太网用的计算机网卡及用于连网的集线器、双绞线电缆及附件，可按 OMRON 要求，从市场上选购。

当然，不是 OMRON 的所有 PLC 都可接入以太网。只是可配置以太网模块或集成有以太网接口的机型才可接入。OMRON 以太网可以是简单的局域网，也可为互联网，还可冗余配置。

1. 以太网模块

OMRON 当前主推的是 CS、CJ 系列及 CP1H 机（可扩展部分连接 CJ 模块）。其以太网模块有 10M 的 CJ1W-ETN11、CS1W-ETN11、CS1W-ETN01，100M 的 CJ1W-ETN21、CS1W-ETN21 等。近期又推出与 EtherNet/IP 兼容，功能又有所增加的 CS1W-EIP21、CJ1W-EIP21、CJ2M-CPU3*、CJ2H-CPU68-EIP 等。这里后缀加 EIP 的模块合乎 Ethernet/IP 标准。用于开放的以太网组网。图 5-30 所示为 CJ、CS 机用的以太网模块的正面视图。

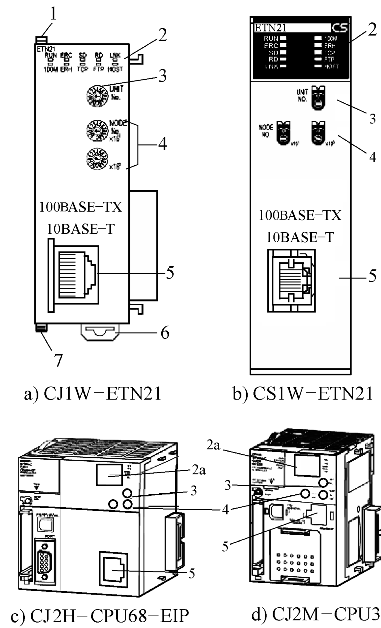


图 5-30　以太网正面外观图
1—用于模块安装的卡脚　2—指示灯
2a—指示灯及 IP 地址　3—单元号设定开关
4—站点号设定开关　5—双绞线连接器
6—模块安装用卡爪

从图知，每个以太网模块面板上都有用以反映以太网工作状态的指示灯、设定单元号及站点号设定开关及 RJ45 双绞线接口。

单元号设定是模块在 PLC 上的唯一标识，是 OMRON PLC 特殊或总线模块使用的传统作法。一旦选定，系统将分配与其相关的内存区（有 CIO 区及 DM 区）供其使用。

使用的 CIO 区为 25 字。其起始地址与单元号的对应关系如下式：

起始地址（字 n） = CIO 1500 + （25 × 单元号）

各个字的功用见表 5-15。

表 5-15　CIO 各个字功用

偏移	位 15～8	位 7～0	数据方向	相关通信服务
n	单元控制开关		CPU 单元到 Ethernet 单元	Socket 服务
n+1	UDP Socket No.1 状态		Ethernet 单元到 CPU 单元	发送邮件功能
n+2	UDP Socket No.2 状态			
n+3	UDP Socket No.3 状态			
n+4	UDP Socket No.4 状态			
n+5	UDP Socket No.5 状态			
n+6	UDP Socket No.6 状态			
n+7	UDP Socket No.7 状态			
n+8	UDP Socket No.8 状态			
n+9	TCP Socket No.1 状态			Socket 服务
n+10	TCP Socket No.2 状态			
n+11	TCP Socket No.3 状态			
n+12	TCP Socket No.4 状态			
n+13	TCP Socket No.5 状态			
n+14	TCP Socket No.6 状态			
n+15	TCP Socket No.7 状态			
n+16	TCP Socket No.8 状态			
n+17	服务状态			FTP 服务等
n+18	出错状态			全部出错条件
n+19	Socket 服务要求开关 2	Socket 服务要求开关 1	CPU 单元到 Ethernet 单元	Socket 服务
n+20	Socket 服务要求开关 4	Socket 服务要求开关 3		
n+21	Socket 服务要求开关 6	Socket 服务要求开关 5		
n+22	Socket 服务要求开关 8	Socket 服务要求开关 7		
n+23	FINS/TCP 链接状态		Ethernet 单元到 CPU 单元	FINS 通信
n+24	（无用）			

使用的 DM 区为 100 字。其起始地址与单元号的对应关系如下式：

起始地址（字 DM） = D30000 + （100 × 单元号）

各个字的功用见表 5-16。

提示：在一台 PLC 中，每个特殊及总线模块所选用的单元号应是唯一的，不能重复。以避免由于不同模块使用同一内存区，而造成混乱。但不必记住这内存区各个字的具体功能。因为在实际上这些字的使用都是用 OMRON 提供的工具软件。

站号是本模块接入以太网的局部地址，也是它在网段中的唯一标识。在网络进一步设定时要用到这个站号。以设置它的 IP 地址及子网掩码。而这个设置可使用编程软件。缺省的 IP 地址为 192. 168. 250. （站号）。如果站号设定值为 01，则默认 IP 地址为 192. 168. 250. 1。

对于 CJ2 CPU 单元，除了指示灯，还有两个 7 段码显示器，可滚动显示 IP 地址。滚动显示 IP 地址完成后，将以十六进制形式显示 IP 地址（ 节点地址）的低 8 位。图 5-31 所示为它的显示过程。这里显示的 IP 地址为 192. 168. 250. 10。其显示过程是，其滚动显示的内

容将按如图方式进行变更。

表 5-16 DM 各个字功用

偏移位	15　　08 07　　00	数据方向	相关通信服务
m	发送邮件状态 1	Ethernet 单元到 CPU 单元	发送邮件功能
m+1	TCP Socket No.1 接收字节数		Socket 服务
⋮	⋮		
m+8	TCP Socket No.8接收字节数		
m+9	TCP Socket No.1连接状态		
⋮	⋮		
m+16	TCP Socket No.8连接状态		
m+17	发送邮件状态 2		发送邮件功能
m+18	Socket 服务参数区 1		Socket 服务
m+28	Socket 服务参数区 2		
⋮	⋮		
m+88	Socket 服务参数区 8		
m+98 m+99	IP 地址显示、设置区	Ethernet 单元到 CPU 单元 或 CPU 单元到 Ethernet 单元	

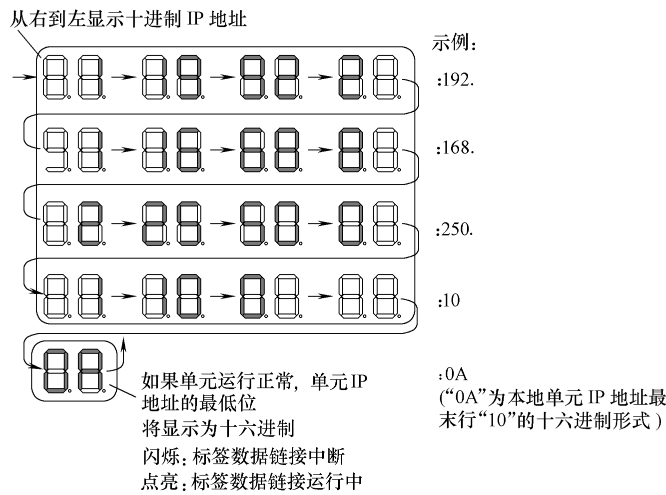


图 5-31　滚动显示过程及最后显示

若网络出错，这两个 7 段码显示器最后将依次显示所有出错代码。以下为错误显示例：

· 与 IP 地址 192. 168. 250. 8 进行通信时发生 d6 错误（无法连接）；

· 与 IP 地址 192. 168. 250. 9 进行通信时发生 d6 错误（无法连接）；

· 与 IP 地址 192. 168. 250. 40 进行通信时发生 d5 错误（校验错误、无目标对象）；

· 内置 EtherNet/IP 端口（192. 168. 250. 10）发生 C6 错误（多开关置 ON）和 EA 错误（EtherNet/IP 扩展设定错误）；

等等。

除了以上以太网模块，OMRON 近期还开发了使 CJ 机的 CJ1W-PNT21 模块，可接入 ProfiNet 工业以太网（见后），可作为 IO 控制器。还有 GRT1-PNT、GRT1-PNT SmartSlice

I/O Coupler 等模块，可作为 Profinet IO 设备站。其目的像 OMRON 公司讲的是，追赶开放标准，以扩大 OMRON 产品的应用范围。

2. 以太网特性

表 5-17 所示为以太网模块 CS1W-ETN21 的主要特性。

表 5-17　以太网模块 CS1W-ETN21 主要特性

项目		规格	
物理层		100Base-TX(也可用于 Base-T)	
站点数		254	
安装位置		CPU 或扩展机架	
可安装单元数		最多 4(含扩展机架)	
传输特性	媒体访问方法	CSMA/CD	
	调制方法	基带	
	传输路径	星形	
	波特率	100Mbit/s（100Base-Tx）	10Mbit/s(10Base-T)
	传输媒体	5 类非屏蔽双绞线(UDP)电缆 5 类屏蔽双绞线电缆(STP)100 欧	3、4、5 类非屏蔽双绞线(UDP)电缆 3、4、5 类屏蔽双绞线(STP)电缆 100 欧
	传输距离	100m(HUB 到站点)	
	层叠连接数	2	4
通过因特网进行 PLC 维修		计算机可使用 PLC 接收邮件功能通过互联网给 PLC 发送命令(含 FINS 命令)	
服务特性		指定 IP 地址或 DNS 代理功能	

从表知，它的站点数可达 254，为基带传输，速率为 100M（可与 10M 兼容）。

3. 以太网连接

OMRON 以太网拓扑为星形，所以，要使用集线器连网。而如果站点较多还可用多个集线器。集线器之间的连接有层叠与堆放两种，如图 5-32 所示。

这里要强调的是，如要使用实时通信，则要选用高性能的交换机。同时，所设定的交换数据量也有所限制。否则难以保证达到预想的要求。

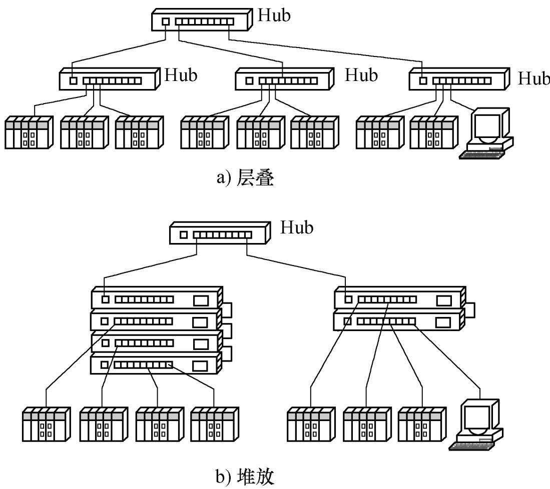


图 5-32　多集线器两种连接

5.4.2　以太网功能

OMRON 以太网特点是高速，现有网速最高可达到 100Mbit/s。并且与计算机网络的兼容性、互联性好。它的功能随版本及所作的设置而有所变化。一般讲新推出的模块功能较强。以下将对其可实现的功能做简要介绍。只是要清楚，不是所有模块都有这么多功能。

1. 在计算机上，使用编程软件 CX-Programmer 直接通过以太网或 USB 口与以太网上的 PLC 通信

这首先要在计算机上，运行 CX-Programmer 软件。运行后建立新工程，在网络类型项设置为 EtherNet/IP。再指定 IP 地址。确定后即可计算机与 PLC 联网通信。图 5-33 所示即为它的设置过程画面。

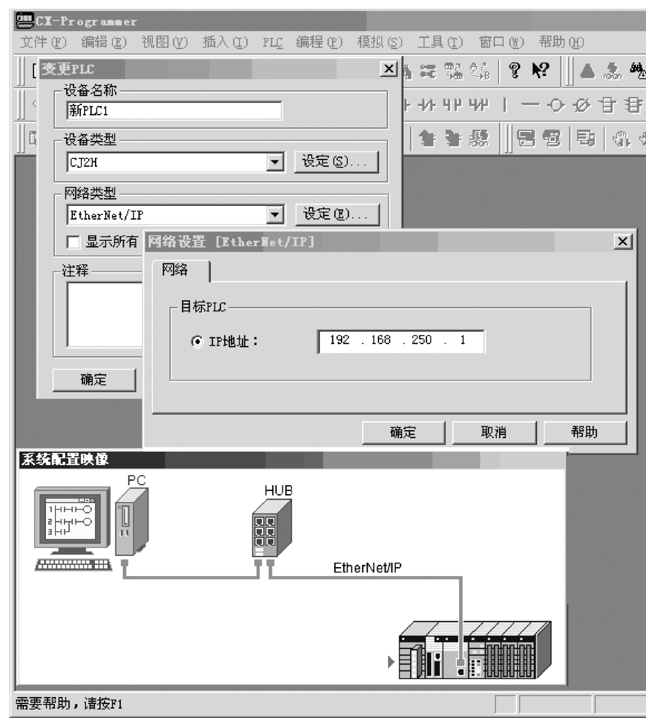


图 5-33　以太网直接通信设置画面

提示：所设置的 IP 地址的网络部分应与计算机的一致，即两者必须同处于一个子网中，否则无法通信。

除了直接通过以太网，也可通过 PLC 的 USB 口，指定该 PLC 连接的以太网上的任一 IP 地址的 PLC，也可与所指定 IP 地址的 PLC 通信。这也称以太网简介通信。图 5-34 所示即为它的设置画面。

如果上述设置正确，PLC 上电后，计算机即可与 PLC 联机。进而上传、下载程序及数据，改变 PLC 的工作模式，监控 PLC 工作。与利用串口与 PLC 联机功能完全相同。而且速度更快，操作的实时性更好。

2. 支持以太网协议及 Socket 的通信服务

支持以太网协议，包括 TCP/IP 与 UDP/IP 在内的国际通用 Internet 协议。同时，还支持 Socket 的通信服务。有了此功能，就可利用 Socket 作为应用接口，可在以太网上实现 PLC 之间，或 PLC 与计算机之间，以至于其他以太网站点直接使用 TCP/IP 与 UDP/IP 协议传送与接收任意数据。

3. 支持文件传输 FTP 协议

利用这个协议，在 PLC 与上位机之间，不需编程就可传输大量数据。图 5-35 所示就是这个数据传输的过程。

从图知，由于以太网单元内装有 FTP 服务器，因而与其连网的计算机可作为客户端访问 PLC。读写安装在 PLC 上内存卡或 EM 文件存储上的指定文件名义进行大量数据交换。

4. 支持 Email 功能

主要指通过同处于互连网上的计算机与 PLC，通过相互发送与接收电子邮件传送数据。



图 5-34　以太网间接通信设置画面

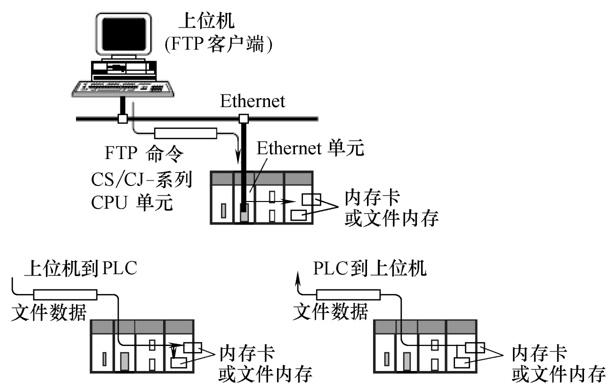


图 5-35　利用 FTP 协议传输数据

图 5-36 所示为在互连网上计算机向 OMRON PLC 发送邮件的示意。与计算机间发送邮件一样，中间也是通过 SMTP 服务器。

PLC 发送邮件由邮件头、邮件体及附件组成。而附件可以是由以太网模块自动生成的 I/O内存数据文件，扩展名为 IOM（二进制）、TXT（文本）或 CSV（逗号隔开的数据文件）。也可是任意在 CPU 单元文件存储器中的文件。但每个邮件附加文件数有限。

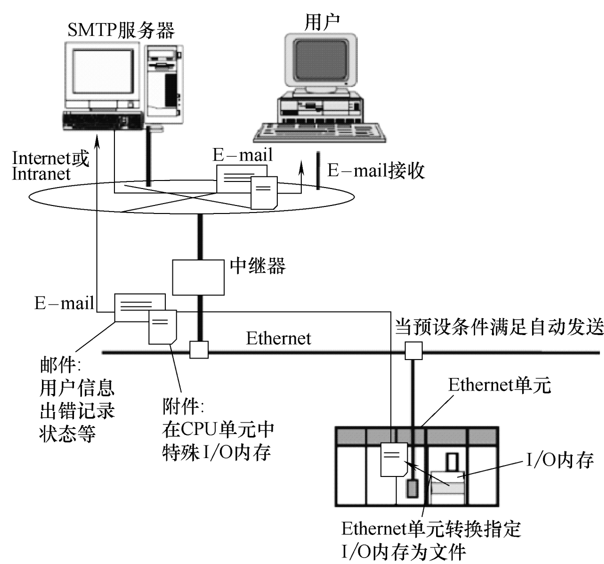


图 5-36 在互连网上计算机向 OMRON PLC 发送邮件示意

图 5-37 所示为加上附件 DATA0. CSV 的邮件传送情况。该附件含有 DM100 ~ DM119200 个字的数据，每个字用逗号隔开。

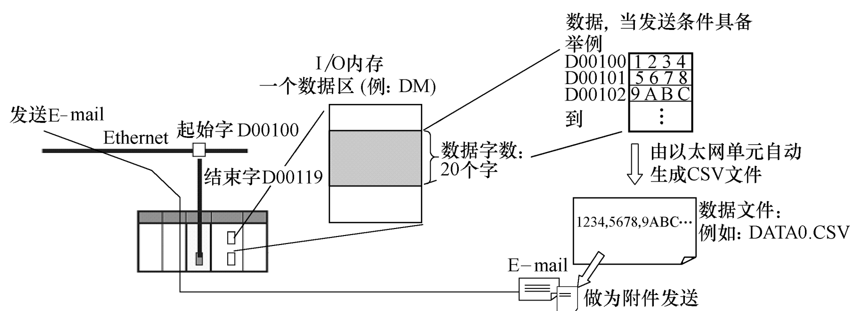


图 5-37 加上附件 DATA0. CSV 的邮件传送情况

PLC 什么时候发送邮件，由相应条件触发。此条件可以是用户设定的 CPU 单元 I/O 内存字段值大小或位的 ON/OFF 变化，也可是 PLC 工作状态变化，也可是定时触发。定时时间可在 10 分钟到 10 天之间设定。任一设定条件满足，都将向指定邮件地址发送邮件。

同样，计算机也可向指定邮件地址的 PLC 发送邮件。图 5-38 所示为 PLC 接收电子邮件的情况。经设定后 PLC 以太网模块会定时检查是否有邮件发来。如果有邮件，即可接收。接收完成后，将向对方发送回复邮件，以确认邮件已收到并回送相应的处理信息。

为了确保安全，可对收取的电子邮件作限定。如只能收取指定地址的邮件，限制对方邮件的命令，只能收取某种扩展名的文件等。如所收邮件不合上述条件，PLC 将不予处理。

OMRON 定义有多个接收的邮件命令。除了上述 FileWrite（文件写）外，还有 FileRead（文件读）、FileDelete（文件删除）、FileList（File List Read）、UMBackup（User Memory Backup）、PARAMBackup（Parameter Area Backup）、IOMWrite（I/O Memory Write）、IOM-Read（I/O Memory Read）、ChangeMode（Operating Mode Change）、ErrorLogRead（Error Log

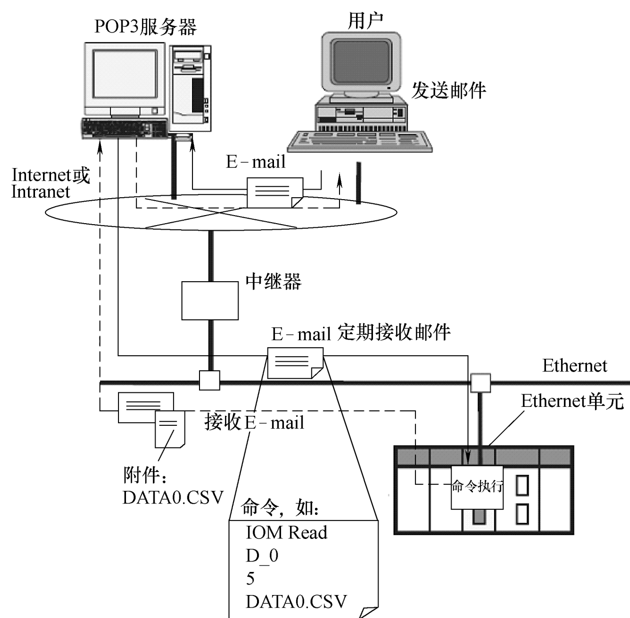


图 5-38　PLC 接收电子邮件的情况

Read）、ErrorLogClear（Error Log Clear）、MailLogRead（Mail Log Read）、MailLogClear（Mail Log Clear）、Test（Mail Test）、FinsSend（FINS Command Send）等。这些命令还都有各的发送与回复格式。但回复码（Respone Code）总是要依据接收邮件的情况自动确定。还要指出的是，由于邮件的数据量较大，所以，传送的时间是较长的。

从上介绍可知，这个电子邮件通信的功能是很强的。使用它可使上位计算机在互连网所覆盖范围内与 PLC 通信，实现与其数据交换及对其实施操作。但这也只是 OMRON 100Base-TX 以太网，并将其接入互连网后，才有此可能。

5. FINS 服务功能

支持 OMRON 公司的标准 FINS 协议，可使用 FINS 通信命令与其他 PLC 交换数据。还可利用 FINS 网关功能，实现与其他网络互连、互通。这些通信命令有 SEND（090）、RECV（098）及 CMND（490）等。可用 PLC 梯形图或其他语言程序执行。

此外，FINS 还是计算机与 PLC 通信的协议。计算机可利用 Socket 接口，与 PLC 按 FINS 协议命令通信。读写 PLC 数据，改变 PLC 工作模式，监控 PLC 系统工作，实现 SCADA 的功能。

6. 自动时钟调整功能

以太网单元可利用以太网上的简单网络时钟协议（SNTP，Simple Network Time Protocol）服务器，获取时钟信息，自动调整 PLC 内装时钟。

7. 指定主机名功能

靠利用域名服务代理（DNS，Domain Name Sever）服务功能，可指定主机名代替 IP 地址用于有关以太网通信。

8. Web 功能

在计算机上，可利用浏览器按设置的权限，对以太网单元进行参数设置与状态监控。可

以设置密码。如未设密码，要先使用缺省的密码“ETHERNET”，然后再更改新密码。

Web 功能也可在编程软件上设置为禁止。

Web 网页访问的地址（URL）是：“http：//（以太网单元 IP 地址）/0”。

9. 支持大容量标签数据链接

这个功能使用的是 EtherNet/IP 的隐形（Implict）通信。使用 EIP 以太网模块或接口组件的以太网才有此功能。组件 EtherNet/IP 网络后，其上的 PLC 与 PLC，或 PLC 与其他相关部件之间不需运行通信程序就可自由地交换大量数据。这个通信机理与 OMRON PLC 的其他数据链接通信本质上也是相通的。所不同的只是，这里用的自定义的标签，而链接用的是 PLC 的内部器件。此外，还可做些更灵活的有关交换数据的设定，如可单独设定各数据链接区的刷新周期，等等。图 5-39 所示为它的通信机理。

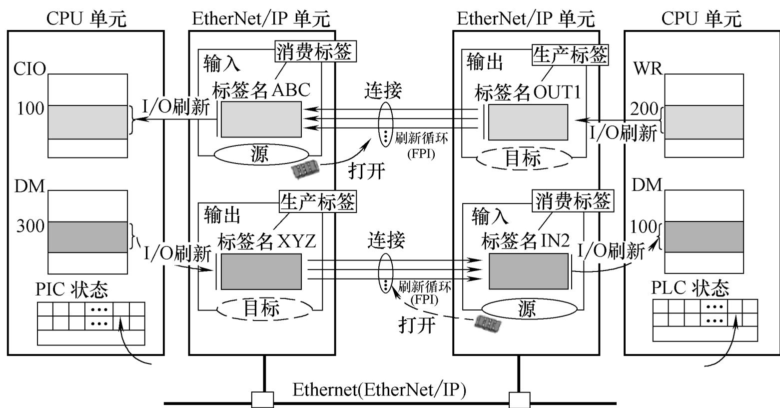


图 5-39　标签链接通信机理

从图知，它也有两个通信过程。一是 PLC CPU 与以太网单元 I/O 刷新。另一是以太网单元之间建立连接后的数据通信。

这里的站点数及可连接数是有限制的。如有的最多可在 256 个站点之间建立 256 个这样连接。每个连接最多可为 722 字，连接总数可达 184322 字，等等。这样连接建立后各方 PLC 无须执行程序，即可交换数据。而且这样连接即使已经建立，且个别站点已运行，也可改变。

5.4.3　以太网设置

要使以太网正常工作，除了硬件安装、接线正确，还要对每个站点的以太网模块做好有关设置。首先是在以太网单元（硬件）上要设好单元号、站号设置。其他就是用编程软件 CX-Programmer 做以太网模块的设置及用 CX-Integrator 做以太网网络设置。

1. 模块设置

模块设置要使用编程软件。在添加模块后在如图 5-40 所示的编辑参数窗口上操作。

这里要设置的项目很多，但最主要的就是设置 IP 地址及子网掩码等。没有设置好将无法与 PLC 通信。模块出厂的缺省的 IP 地址是：192. 168. 250. 站号。初次使用此模块可使用这个地址。重新设置这个当然可以，但建议所设置的 IP 地址最后一个字节最好与站号一致。

这样做便于用自动生成模式（动态/静态）转换 IP 地址。



图 5-40　TP 地址设置窗口

除了上述 IP 地址设置，还有模块实现功能的设置。这些设置当然与选用的模块有关。图 5-41 所用模块为 ETN11，功能少。除了基本设置，就是邮件设置。图 5-41 所示就是它的邮件设置。



图 5-41　邮件设置

从图可知，这里要指定自身地址，通信对方地址以及邮件服务器 IP 地址等。如果选用功能强的模块如图 5-42 所示的 ETN21 模块，那要设置的选项就很多。如图所示选在“HT-TP”页面设置。目的是使用 Web 服务器功能。



图 5-42　ETN21 模块 HTTP 设置选项

从图知，本例设置为使用 WEB 功能。缺省密码“ETHERNET”改为“OMRON”。正如前已述及，这个改动也用浏览器实现。其他设置选项还很多，多关于互联网的有关设置，这里不多赘述。

提示：上述设置也可通过 I/O 登记自动实现。这也是 OMRON PLC 所特有的。

2. 网络设置

对一般以太网单元使用集成在 CX-ONE 软件包中的 CX-Integrator 软件就可进行设置。可先脱机创建网络，再添加站点，并对站点做设置。之后，计算机可与其连网，监测网络。其过程与 OMRON 其他网络设置类似。

而对 EtherNet/IP 模块则要、可使用 EtherNet/IP 网络配置器（Network Configurator For EtherNet/IP）专用软件进行标签数据链接设置。此软件也集成在 CX-ONE 中，安装好 CX-ONE 也可打开此软件。

3. 标签链接设置

这个设置要同时运行 CX-Programmer 及 Network Configurator For EtherNet/IP 两个软件。集体设置步骤如下：

（1）建立 EtherNet/IP 网络，添加以太网站点

运行 Network Configurator For EtherNet/IP，创建新工程。在 Network Configurator 窗口上用鼠标拖放相关 EIP 站点图标到网络上。建立 EtherNet/IP 网络。图 5-43 所示为 3 个站点网络。并分别指定了 IP 地址。

（2）添加网络变量

运行 CX-Programmer 编程软件，创建新工程。添加所有网络中的 PLC，做好 I/O 配置。如 PLC CPU 没有集成 EIP 接口，要添加 EIP 模块。并做好设置。所设置的 IP 地址要与建网的一致。进而在每个 PLC 的符号表上添加网络变量。其做法是，用鼠标右键点击全局符号表，在弹出的菜单中选“插入符号”项。之后将弹出图 5-44 所示的“编辑符号”小窗口。

如图所示，要先使网络变量激活，然后再公布、输入、输出 3 项中选一个。该图时针对 PLC1，变量名为 px1 的网络输出标签（Tag）。从图下角知，这里还有 px2、px3 为它的网络输出标签（Tag）。除了名，还指定了相应的 PLC 内部器件名称，如图用 D10。

提示：只有添加的 PLC 配置有 EIP 接口或模块，“编辑符号”小窗口才显示有网络变量

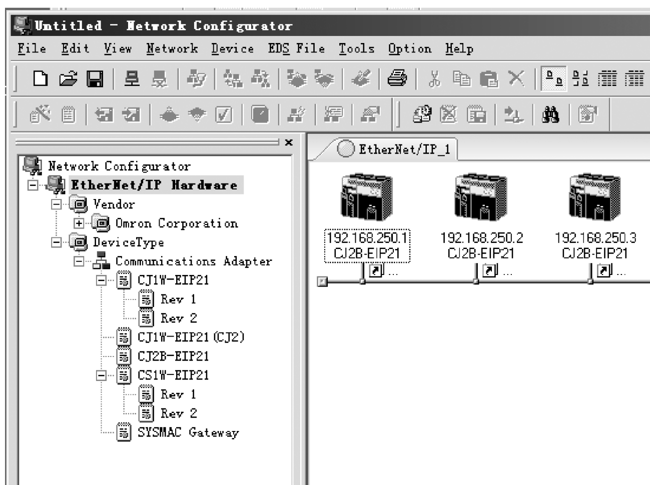


图 5-43　3 个站点 EtherNet/IP 网络结构



图 5-44　“编辑符号”小窗口

选项，才可做网络变量编辑。

除了选择输入、输出，还可选择公布。选它可允许外部部件访问。

网络上所有参与链接的 PLC 都要添加网络变量。从图还可看出，网络变量与其他 PLC 全局变量的图标是有差别的。以上工作完成后，别忘了存储文件。

（3）读入网络变量，做好站点参数编辑

这时 CX-Programmer 软件还要继续运行，但令其最小化。同时转过来激活图 5-43 所示窗口。双击其上站点图标，将弹出编辑站点参数（Edit Divice Parameters）窗口。如图 5-45 所示。这时，再点击该图右下方“Inport”按钮，之后按提示操作，将把在 CX-Programmer 中添加的网络变量加入到表中。

从图所示可知，这里加入了是站点 1（PLC1）的 2 个网络输入变量（px2、px3）。还有 px1 为输出变量，点击“Out Produce”标签后也可显现。

同理，也可对站点 2、3 做相同操作。也做好它的参数编辑。

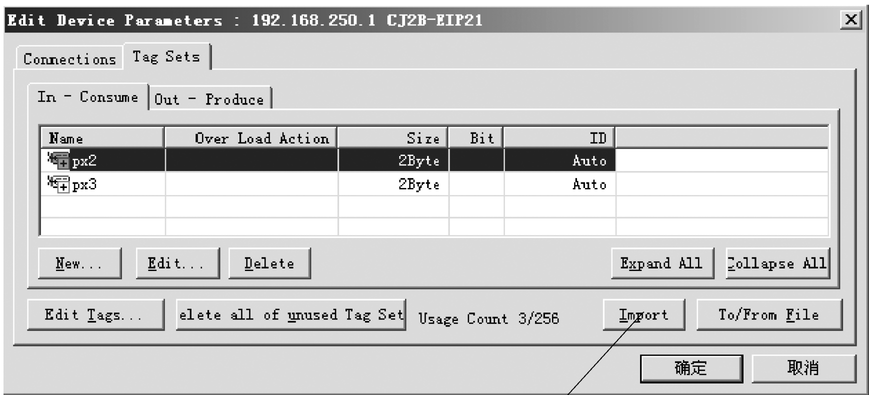


图 5-45　站点 1 读入的网络变量

（4）建立连接

设置好输入、输出标签之后，要对链接的源站点（这里为输出站点）做连接设置。每个连接要指定名称、与其连接的目标站点及链接的输入输出对应标签。具体办法是：

1）点击站点编辑参数窗口上的连接标签（Connections），将出现图 5-46 所示连接窗口。在此窗口上部显示待连接的两个目标站点。

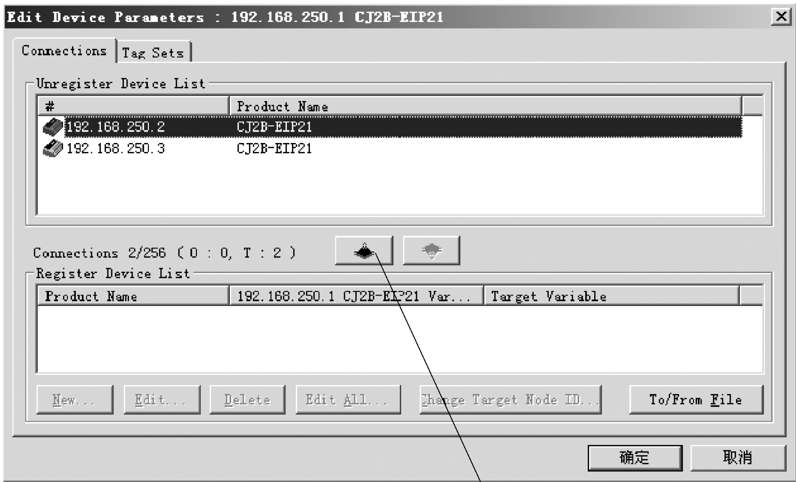


图 5-46　连接窗口

2）点击图示按钮，把该窗口上的待连接站点移入登记部件列表（Register Device List）中。

3）选定一个登记部件列表站点，用鼠标双击之。将弹出图 5-47 编辑连接窗口。

这时，在目标部件（Target Device）小窗口中的输出标签集（Output Tag Set）中选站点 2 的输出标签，如图为 px2。在源部件（Originator Device）小窗口中的输入标签集（Input

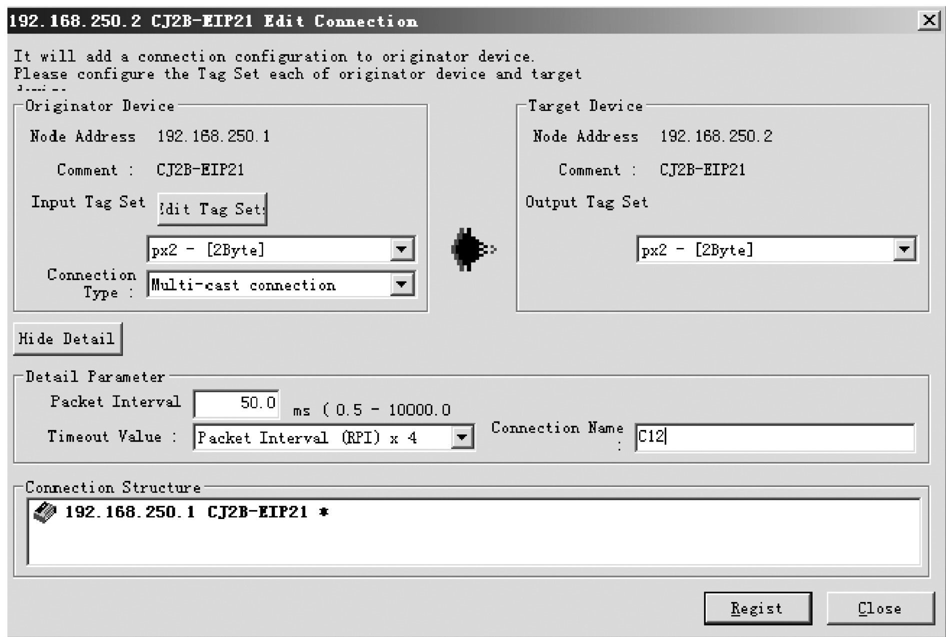


图 5-47　编辑连接窗口

Tag Set）中选站点 1 的输出标签，如图也为 px2。再输入连接名称，这里为 C12，含义为站点 1 与站点 2 之连接。此外，还要对数据包的发送间隔（Packet Interval）做设置。根据应用要求及标签值实际变化情况，可在 0.5 ~ 10000ms 之间选择。本例按缺省选 50ms。再就是发送出错时间也缺省选定为选定为 RPI 的 4 倍。超过此设定时间将出错报警。全部选定后点击“Regist”按钮，予以登记。如还有其他连接，还可接着设置并登记。

所有相关连接都逐一设置，并登记后，点击“Close”按钮，退出此窗口，又回到连接窗口。这时，如点击其上的“Edit All”按钮（该图此按钮未激活，如果已登记连接，此按钮将激活），可弹出如图 5-48 所示的编辑全部连接（Edit All Connections）窗口。还可在其上做些参数更改，或再增加编辑项。

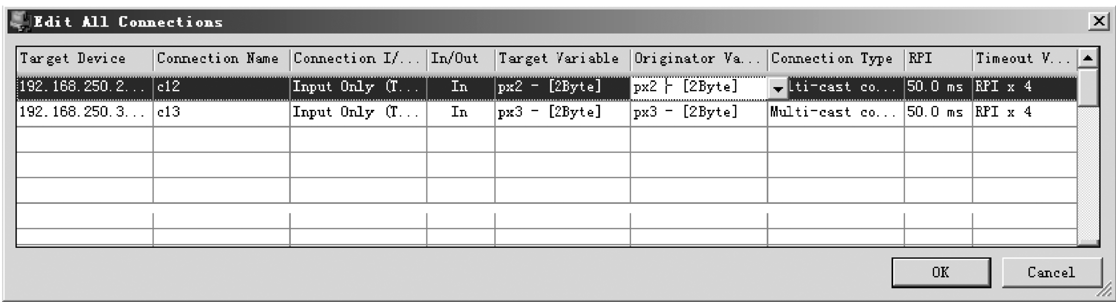


图 5-48　编辑全部连接窗口

4）站点 1 与站点 3 的连接也照此办理。还有就是站点 2、站点 3 的相关连接也要处理。

全部连接完成后，在 EtherNet/IP 网络结构窗口上，可点击“Network”、“View Device’s Connection Structure Tree”菜单项，可弹出连接结构树窗口看到整个连接的情况。图 5-49 所示就是本例的连接结构树。

此时，在 EtherNet/IP 网络结构窗口上，可点击“Network”、“Check Connection”菜单项，检查连接是否有误。本例显示“No Connections Error Found”。说明连接无误。可以往下继续设置。

(5) 检查带宽利用率

在网络结构图上，点击“Detail”按钮，将弹出部件带宽利用率窗口。可观测所作的连接带宽利用情况。图 5-50 所示为本例连接带宽利用的情况。

从图知，本例带宽是蛮有富裕的。连接多时，可能紧张的情况。这时也许要做些调整。如加大 RPI 时间等。

(6) 下载设置

脱机做好以上设置，即可联机，并下载上述所有设置。联机后也可上载这些设置。

(7) 起动或停止链接

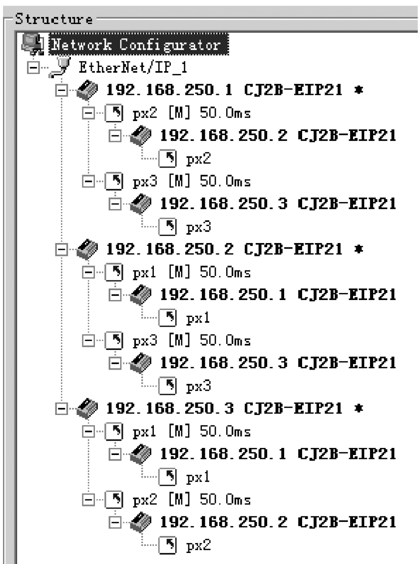


图 5-49 连接结构树窗口

在 EtherNet/IP 网络结构窗口上，可点击“Device”、“Monitor”菜单项，并选定“Connection”表单，可显示如图 5-51 所示监控部件窗口。

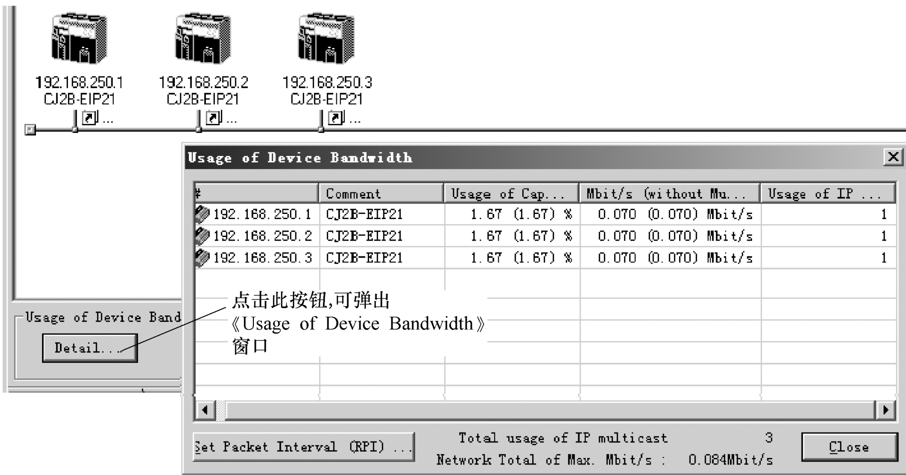


图 5-50 本例连接带宽利用情况

在其上可点击“Start Connection”按钮，起动连接。也可点击“Stop Connection”按钮，停止连接。选定此窗口的其他表单，还可做其他监控。

以上只是对使用以太网模块设置的简要介绍。还有不少细节，可参阅有关说明。

5.4.4 以太网配置实例

1. 简单连网

图 5-52 所示为简单以太网配置。有一台计算机及两台 PLC。前者用以太网卡，后者用以太网模块，用双绞线，通过集线器相连。连网后可实现计算机分别与两台 PLC 通信，也可实现两台 PLC 键通信。

这样联网可用以实现计算机对 PLC 的编程及监控（SDADA 功能）。同时，两台 PLC 还可使用 FINS 通信命令进行数据交换。是很常见的配置实例。

2. 复杂连网

图 5-53 所示为 PLC 以太网与企业内部网（Intranet）相接，同时，企业内部网还通过防火墙、IP 路由器服务器接入互联网。在这个 PLC 以太网上，计算机与 PLC 相互可以通信，与企业内部网络上的其他站点也可通信。只要防火墙允许，还可通过互联网与企业外部的计算机通信。

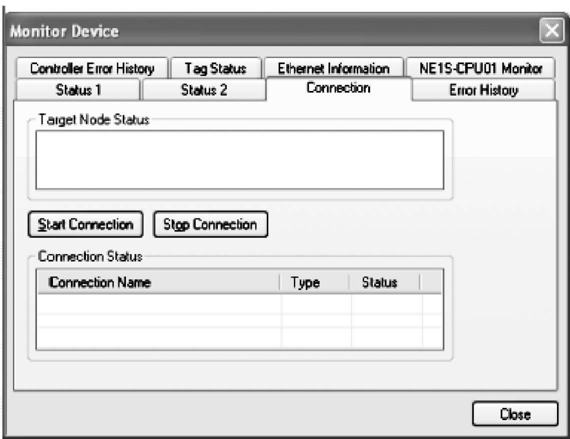


图 5-51　监控部件窗口

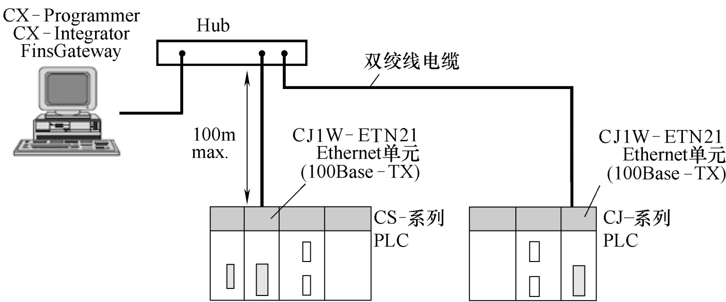


图 5-52　简单以太网配置

这样联网可实现的功能更多。既可用以实现计算机对 PLC 的编程及监控（SDADA 功能），两台 PLC 还可使用 FINS 通信命令进行数据交换。同时，PLC 还可接入互联网，实现普通互联网站点可实现的功能。进而把 PLC 控制系统从封闭走向开放。

3. 冗余配置

图5-54 所示为冗余配置的 PLC 以太网。PLC 用的为 CS1D 机，有两个以太网模块。计算机也有两个以太网模块，分别通过 Hub 相接。这里一个为主，另一个备份。可确保通信万无一失。

这样联网主要是为网络安全、可高考虑。可确保 CS1D 冗余功能得以更好的实现。

4. 标签链接配置

图 5-55 所示为 10 台 CS1W-EIP21 单元以及 10 台 CJ1W-EIP21 单元配置成的标签链接以太网。每个站点有 100 个字标签用以发送数据，有 1900 个标签用以接收数据。因此，各站点之间都可相互进行数据交换。

这里要求数据包发送的时间间隔（Requested Packet Interval，RPI，以 0.5ms 为单位在 0.5 到 10000ms 之间设置）为 10ms。站点的 IP 地址设置范围从 192.168.250.1 ~ 192.168.250.20。其数据交换示意如图 5-56 所示。

用网络配置软件观测得知，这时的带宽利用率（Usage of Capacity）为 39.67%。详细如图 5-57 所示。

可看出，这里各站点的 RPI 都是 10ms，带宽利用率也都是相同的。其实可以点击上图“Set Packet Interval（RPI）”按钮，将弹出相应窗口，再做进一步设定，改变此值，以至于各个站点分别还有不同的 RPI 设置。

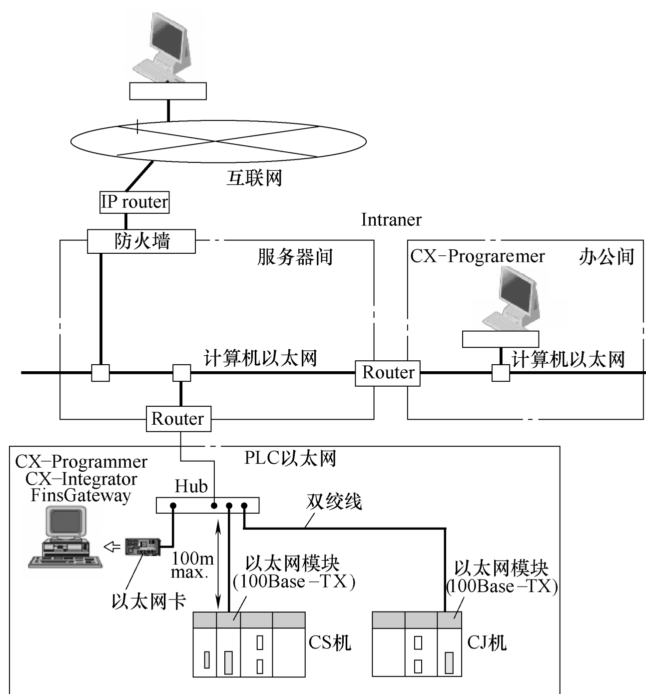


图 5-53　互连以太网

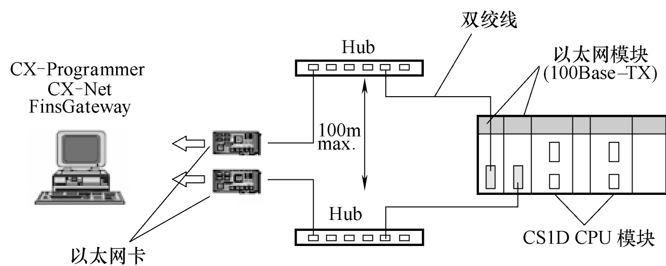


图 5-54　冗余配置 PLC 以太网

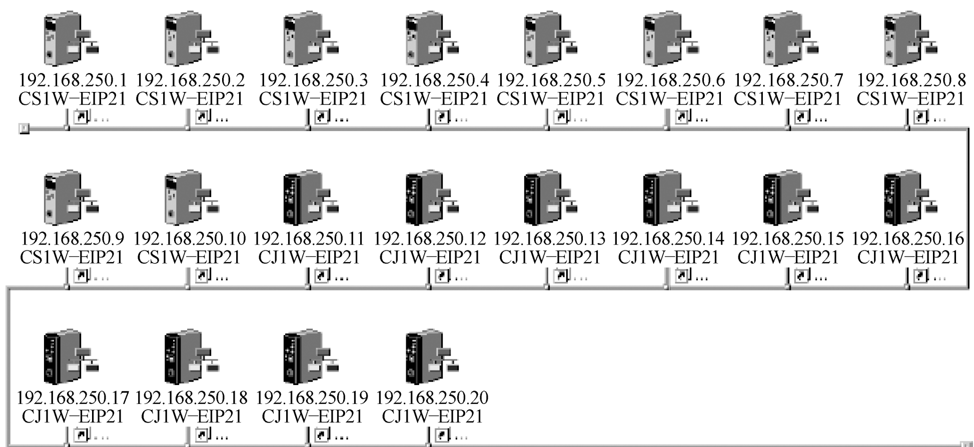


图 5-55　标签链接以太网

IP 地址 192.168.250.1　192.168.250.2　192.168.250.3　…　192.168.250.20

CS1W-EIP21　CS1W-EIP21　CS1W-EIP21　CJ1W-EIP21

100个字　传送

100个字　传送

100个字　传送

100个字　传送

标签数据链接区（100 个字×20 单元）

10 个 CS1W-EIP21 单元 +10 个 CJ1W-EIP21单元=20个单元

所有连接的 RPI 为10ms（以太网缺省）

图 5-56　20 个站点数据标签数据交换示意

Usage of Device Bandwidth

#	Comment	Usage of Cap...	Mbit/s	Usage of IP m...
192.168.250.1	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.2	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.3	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.4	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.5	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.6	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.7	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.8	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.9	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.10	CS1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.11	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.12	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.13	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.14	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.15	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.16	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.17	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.18	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.19	CJ1W-EIP21	39.67%	4.837Mbit/s	1
192.168.250.20	CJ1W-EIP21	39.67%	4.837Mbit/s	1

Set Packet Interval (RPI) ...　Total usage of IP multicast addresses : 20　Close

图 5-57　网络带宽利用率

5.5　西门子 PLC 以太网配置

关键词：I/O 控制器、I/O 设备、基于以太网、存储转发、可缩放通信、RT、IRT、集成交换机

西门子 PLC 以太网有传统的以太网及开放的 ProfiNet 工业以太网。本节主要介绍 ProfiNet 工业以太网。

5.5.1　Profinet 简介

Profinet 由 Profibus 国际组织（Profibus International，PI）推出的新一代基于快速以太网技术的、开放的自动化总线标准。已集成全双工切换技术，并已进行了标准化。涵盖实时以太网、运动控制、分布式自动化、故障安全以及网络安全等技术，可实现管理层与现场总线系统的无缝集成与通信的连续性，为自动化通信领域提供了一个完整的网络解决方案。

ProfiNet 以交换机为网络架构的核心。所以从狭义上说，ProfiNet 就是工业以太网中的一个协议。而从广义来说，当网络设备通信使用 ProfiNet 协议时，这个网络就可以称作 ProfiNet 网络。

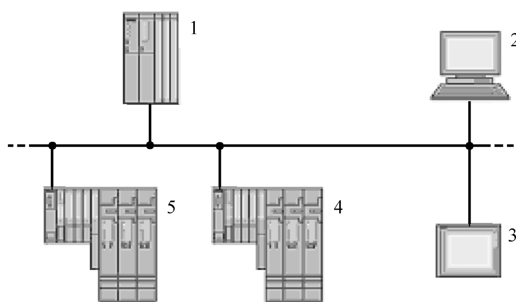


图 5-58 ProfiNet IO 系统组成
1—IO 控制器 2—PG（编程设备）/PC（计算机）
3—HMI（人机界面） 4、5—IO 设备

1. ProfiNet 组成

图 5-58 所示为 ProfiNet IO 系统组成。

从图知，其组成站点有：IO 控制器（Profibus 对应称之为主站）、编程设备/PC、ProfiNte/工业以太网、HMI（人机界面）及 IO 设备（Profibus 对应称之为从站）等。

（1）IO 控制器

一般为 PLC，可运行程序，实施对 IO 的管理与控制。

（2）IO 设备

为分散的现场设备，可分配给某个 IO 控制器管理，接受其控制。其组件一般由接口及 IO 模块组成。IO 模块有具体通道，IO 数据可在这些通道中读入和读出。接口模块从 IO 控制器接收数据，并通过总线将数据传给其他的模块；接口模块也从其他的模块接收实时和诊断数据，并把这些数据传给 IO 控制器。每个 IO 设备都有一个唯一的设备识别号，该识别号在 ProfiNetIO 框架内分配。识别号有 32 位：16 位生产商识别号，16 位设备识别号。生产商识别号由 Profibus 用户组织（PNO）分配。

如同在 Rrofibus，它的设备也有描述文件，以便于把 ProfiNet 设备集成到一个 IO 控制器的组态工具中。IO 设备的属性以 GSD（General Station Description）文件的形式描述，该文件包括下面必需的信息：IO 设备属性（如通信参数）；可嵌入的模块（类型数）；独立模块的组态数据；模块参数；记录诊断错误的文本（如断线、短路。与 Profibus 的 GSD 不同的是，它用的语言不是 ASCII 语言，而是 XM（扩展的标记语言）语言。

（3）监视器

具有投运和诊断功能的编程装置/PC。

（4）HMI

人机界面，用以监控系统工作。

此外，还有有源网络组件（例如交换机、路由器）及到 Rrofibus 等的代理器（网关），以便把这些网络也集成到 ProfiNet 通信中。

图 5-59 所示为较复杂的 ProfiNet 网络组成。该图注明有各个站点的名称。

从图知，它上通过防火墙与广域网相连，下通过种种交换机与现场设备相连。根据安全及实时的要求，具有不同的级别。如图所示，有：办公级别，用于企业的办公管理层；MES（制造执行系统）级别，用于制造管理层；产品，即部件级别，用于现场层。而其中的保护区，则为了确保网络安全而用。

2. ProfiNet 协议模型

ProfiNet 协议实际上是一个由多种协议组成的协议集合，包括 DCP、TCP/IP、UDP/IP、PN IO、PN CBA、PN IRT 等等。ProfiNetRT 在 ISO/OSI 的 7 层堆栈结构中做出重大变化，去

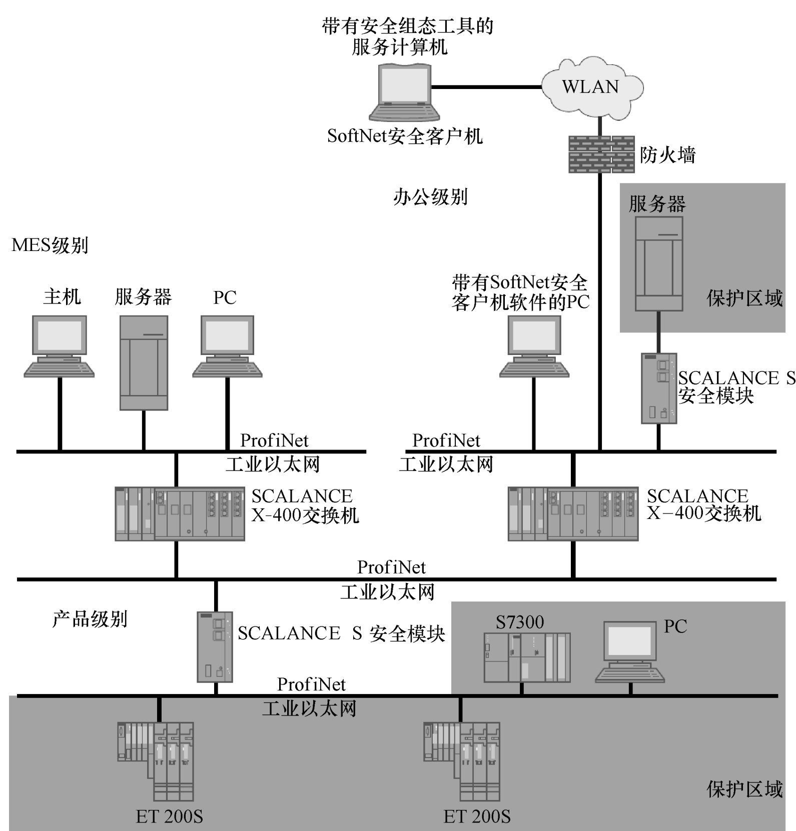


图 5-59　较复杂的 Profinet 网络组成

除 TCP/IP，只保留第 7 层应用层的数据。这样，数据在打包和解包过程中，可直接进行应用层和物理层之间交换。其目的就是尽量减少数据在通信堆栈中打包和解包时间，保证数据在最短时间内完成数据交换。

目前，Rrofibus 已经成为中国第一个工业通信领域现场总线技术国家标准。ProfiNet 成为国家指导性文件。

3. ProfiNet 总线访问方法

ProfiNet 总线访问使用交换以太网，由点对点连接组成。其中每个设备直接与一个（且只有一个）其他设备相连。所使用交换机可同时进行双向通信（发送和接收）。这样，可以使网络容量达到 200Mbit/s，或者达到快速以太网带宽（100Mbit/s）的两倍。由于使用为 ProfiNet 规定的交换技术，因此在 ProfiNet 上进行数据传输不会发生冲突。

在 ProfiNet 中，SIMATIC（西门子）的交换机通过以下两个机制满足实时属性：存储转发和切入。

（1）存储转发

在此过程，交换机会存储报文，并将它们排成一个队列，如图 5-60 所示。然后，报文

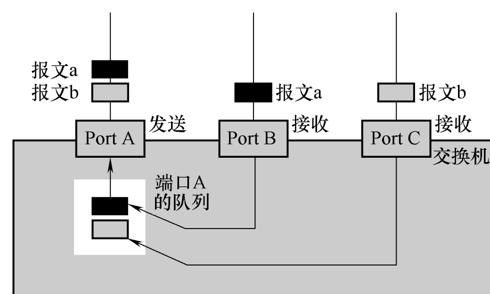


图 5-60　存储转发

将选择性地转发到可以访问已编址节点的特定端口。这里的存储只是临时的，而且也仅当目标端口与下一个交换机的端口之间的区段已被占用时才会出现。

（2）切入

在切入过程中，并不是将整个数据包临时存储在缓冲区中，而是在读取前 6 个字节（目标地址）后，马上直接将其传送到目标端口。因此，数据包通过交换机所需的时间就会减至最少。

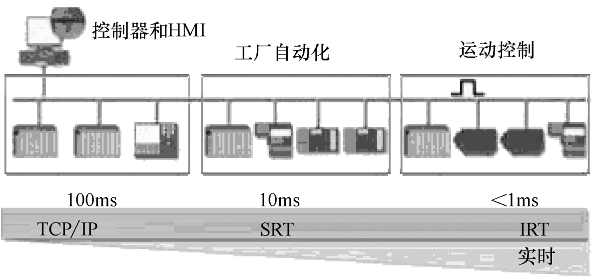


图 5-61　可缩放的通信

4. ProfiNet 通信

ProfiNet 通信如图 5-61 所示，采用基于以太网，在一根线上可同时进行从一般性能到高性能和时间同步的可缩放的通信。这 3 种通信覆盖了自动化应用的全部范围，确保了直至企业管理层的一致性和自动化过程中的快速响应时间。表 5-18 所示为这 3 种通信的相关特点。

表 5-18　3 种通信相关特点

功能	信息集成或过程自动化	工厂自动化	运动控制
通信技术	DCOM	ProfiNet I/O	ProfiNet IRT
通信周期/ms	≥100	10	<10
OSI 层 3～4	TCP/IP	TCP/IP + RT protocols	TCP/IP + IRT protocols
OSI 层 1～2	Standard Ethernet	Standard Ethernet	SpecializedIC

（1）使用 TCP/UDP 的标准通信

ProfiNet 使用以太网和 TCP/UDP/IP 协议作为通信基础。但 TCP/UDP/IP 只提供了使以太网设备能够通过本地和分布式网络的透明通道中进行数据交换。因此，在较高层上则需要其他的规范和协议（亦称为应用层协议），而不是 TCP/UDP。所以，只有对于所有设备都使用相同的应用层协议时，才能保证互操作性。典型的应用层协议有：例如 SMTP（用于电子邮件）、FTP（用于文件传输）和 HTTP（用于互联网）等。

ProfiNet 通过 TCP/UDP 和 IP 的标准通道，发送非苛求时间的数据，例如：参数、组态数据和互连信息，以满足自动化层与其他网络（MES，ERP）的连接需求。尽管其响应时间大概在 100ms 的量级，不过，对于工厂控制级的应用来说，这个响应时间就足够了。

（2）实时（Real-Time，RT）通信

对于生产装备内苛求时间要求的数据的传输，其响应时间要小于 10ms。为此，ProfiNet 采用一个优化的、基于以太网第二层（Layer 2）的实时通信（软实时）通道。显著地减少了通信栈所占用的运行时间，从而提高了过程数据刷新速率。这一方面，由于若干个协议层的去除，可减少了报文长度；另一方面，在需要传输的数据准备就绪发送（即：应用准备就绪处理）之前，也只需较少的时间。同时，还可简化设备用于通信的处理。此外，为获得更佳的效果，ProfiNet 中的数据包还按照 IEEE802.1Q 规范，分配传输优先级，最多可用到 7 级。设备之间的数据流由网络组件依据此优先级处理。优先级 6（Priority 6）就是用于实时数据的优先级。图 5-62 所示为 ProfiNet RT 通信协议及其帧结构。

（3）等时同步实时（Isochronous Real-Time，IRT）



图 5-62　ProfiNet RT 通信协议及其帧结构

上述解决方案对于运动控制应用还远远不够。运动控制应用要求刷新速率在 1ms，100 节点的连续循环的抖动精度为 1m。为此，ProfiNet 在第二层上定义了如图 5-63 所示的 IRT 时间槽及其帧结构，以控制数据传送。

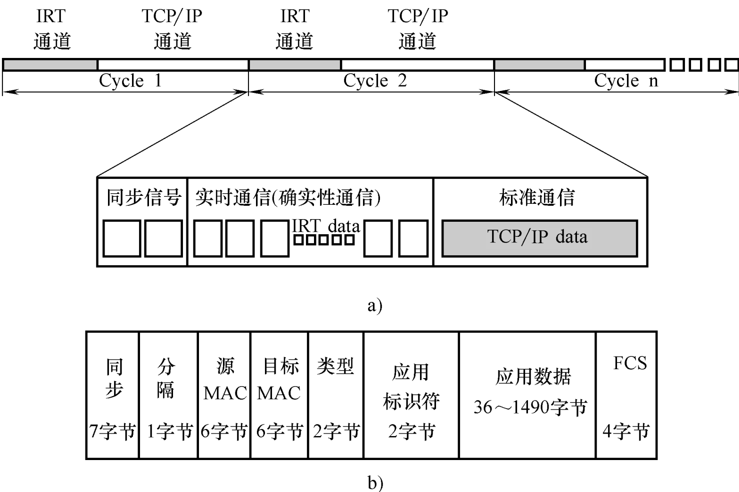


图 5-63　Rofinet IRT 时间槽及其帧结构

从图 5-63a 知，它的通信周期主要分成两个部分，即：时间确定性通信和开放通信部分。之前还有同步化信号。循环的实时报文在 IRT 通道中传输，而其他的报文则在 TCP/IP 通道中传输。这种处理方法可与高速公路媲美，最左边的车道总是为时间要求最紧迫的车辆（实时通信）而保留的，由此防止其他车道上的用户（TCP/IP 通信）占用此车道。甚至在右边车道交通拥塞的情况下也绝不能影响时间要求紧迫（苛求时间）的车辆的交通（通信）。

这里的等时同步数据传输用的是硬实时 HRT（Hardware RT）方案。其实时性是基于一个建立在快速以太网 Layer2 上的时间触发（time-triggered）协议，由内嵌的 Switch-ASIC 同步实时交换芯片保证。这可进一步缩短通信栈软件的处理时间，特别适用于高性能过程数据的等时同步传输及快速的时钟同步运动控制。由于它基于硬件实现，IRT 帧中通常无需 RT 帧中的 IEEE802.1Q VLAN 标识。其帧结构如图 5-63b 所示。

以上 3 种通信的关系是：除了在更新时间内为 IRT 通信保留了带宽外，在更新时间内还允许进行 RT 通信和 TCP/IP 通信。在 RT 通信中，将在 IO 控制器和 IO 设备之间传输循环数据，但是，无法获得“最佳的同步效果”。未同步的 IO 设备将使用 RT 通信自动交换数据。

5. Profinet 功能

（1）IT 服务功能

1）TCP 服务。与可发送和接收数据的任何通信伙伴（例如 PC 或非 Siemens 系统）通

信。可将连续不断的数据块（最大 8KB）从一个以太网节点传送到另一个以太网节点。数据的接收由通信伙伴进行确认。TCP 服务通过以下两种机制来确保数据传输及数据完整性：传输出错时重复发送数据；接收器通过循环算法（CRC）检查已传送数据的完整性并确认数据的接收。

2）UDP 服务。UDP（用户数据报协议）支持可发送和接收数据的任何通信伙伴（例如 PC 或非 Siemens 系统）通信。UDP 为无需确认的简单跨网络数据传输提供通信服务。可在 IP 上将连续不断的数据块（最大 2KB）从一个以太网节点传送到另一个以太网节点。由于不发送任何对所接收数据的确认信息，所以 UDP 帧并不可靠。

3）其他服务。与 FTP 通信（文件传输协议）、SMTP（简单邮件传输协议）、SNMP（简单网络管理协议）及 HTTP（超文本传输协议）等协议有关的服务。可用以传输文件、邮件、网络管理（包括用于监视、控制和参数化网络节点）及创建网页，让联网计算机可通过浏览器访问。当然使用这些服务要求配置有与此功能相应的以太网接口或模块。

（2）控制器相互通信功能

这点与其他控制或信息网络一样，在网络上的各个 IO 控制器站点均可相互通信，交换数据。

（3）PG/PC 站点可对网络进行组态、诊断，对 PLC 站点进行、编程及监控

HMI 站点也可监控网络其他控制站点。

（4）ProfiNet IO 控制功能

通过网络科实现 IO 控制器对远程的 IO 设备交换数据实施控制。其通信可在非实时（NRT）、实时（RT）及等时实时（IRT）之间选择。

（5）现场总线集成功能

可通过代理服务器把其他现场总线如 Rrofibus DP 无缝集成到 ProfiNet 上。从而实现一个从已有的工厂单元到新安装的工厂单元完全透明的转换。

（6）其他功能

如 CBA（Component Based Automation）、OPC、PROFIdrive 及 PROFIsafe 等功能。

6. ProfiNet 拓扑结构

Profinet 网络拓扑有：星型、线型、树型和环型。而实际系统多是由混合结构组成。这些结构可用通信介质有铜缆或光缆。

（1）星型

如果将通信节点连接到具有两个以上 ProfiNet 接口的交换机，则自动创建星型网络拓扑。与其他结构不同，星型结构中的单个 ProfiNet 设备发生故障不会自动导致整个网络发生故障。仅当交换机发生故障时部分通信网络才会发生故障。

（2）树型

如果将若干星型结构互连，则可获得树型网络拓扑。

（3）线型

所有通信节点连接在一个线型总线上，是通过已集成在 ProfiNet 设备中的交换机来实现。需要的接线工作最少。但是，如果一个连接元件（例如交换机）发生故障，则通过该故障连接元件建立的通信无法再进行下去。

（4）环型

如果要增加可用性，则应使用环型结构。将网络的两个开放端连接到一个交换机即可获得环型结构，然后可以将该交换机作为冗余管理器进行操作。如果网络中出现断路，冗余管理器将确保在一个完好网络连接中重定向数据。特定的 SCALANCE X 产品系列交换机默认设计为冗余管理器。也可 STEP 7 中工程工具端口的“属性”对话框中为各个端口配置冗余管理器功能，前提是交换机支持该功能。

7. ProfiNet 网络组件

ProfiNet 有无源网络组件和有源网络组件：如电源线和插头连接器属于无源网络组件；如交换机、接入点、客户端模块、介质转换器和连接模块属于有源网络组件。表 5-19 所为 ProfiNet 的常用到各种网络组件。

表 5-19　ProfiNet 常用网络组件

介　质	组　件	注　释
铜缆(电气)	交换机	用于在工业以太网中互连节点 用于耦合两个网段
	中继器	用于将 ProfiNet 耦合到 Profibus
	PN/DP 连接器	用于耦合两个 PROFINET 子网
	PN/DP 连接器	用于耦合各种不同介质的网络
	介质转换器	
	SCALANCE X	用于连接节点和建立电气网络
光纤导线(光纤)	SCALANCE X	用于连接节点和建立光网络 用于连接节点和建立光网络
无线电(无线)	接入点	用于近距离无线传输
	IWLAN/PB 连接器 PN IO	用于将工业以太网无线耦合到 PROFIBUS DP

8. ProfiNet 技术规格

表 5-20 所示为 Profibus 技术规格。

表 5-20　Profibus 技术规格

标准	符合 IEEE 802.3u 的以太网
传输速率	110/100Mbit/s
站的数量	不受限制
网络规模 · 交换机网络 传输速率 100Mbit/s	无限制(超过 150km,应注意信号传输延迟)
传输介质 · 电气网络 · 光纤网络 · 无线网络	 工业双绞线和双绞线 光纤(玻璃) 环境空间
拓朴结构	总线,树形,冗余环,星形
协议	与协议无关

9. ProfiNet 特点

1）基于以太网，可以利用以太网组件，分享以太网技术进步成果。且具有切换技术的可升级性能。

2）适用不同环境，可按需要做适合不同应用环境的配置。可使不同应用区域（例如办公区域和生产区域)。

3）可自动侦测、识别与适用于传输速率。

4）可无缝集成，覆盖多种网络。使用代理可将现有的现场总线系统（例如 Profibus、ASI 等）集成到 ProfiNet 中。这样，就可建立由现场总线和基于以太网的子系统组成的混合系统，从而实现向 ProfiNet 技术的连续过渡。

5）可冗余配置，提高网络的可靠性。

6）拓扑结构灵活，有多种通信介质可选，例如，工业双绞线、光纤导线以及无线介质。

7）可使用运动控制（ProfiDrive）和故障安全（ProfiSafe）应用技术。

8）可使用具有自治能力的技术模块。其优点是：技术模块可预组装；技术模块可预测试；技术模块可容易地重复使用；通过并行地进行模块建立，相当可观地减少投运时间；可降低成本；能很快和很容易地由各种标准模块组态出客户化的机器/成套系统。

5.5.2 西门子以太网组件

SIMATIC NET 工业以太网有两种类型，分别为 10Mbit/s 工业以太网和 100Mbit/s 工业以太网。它是利用带传输技术，基于 IEEE802.3 利用 CSMA/CD 介质访问方法的单元级和控制级传输网络。在西门子工业以太网中，通常使用的物理传输介质是屏蔽双绞线（TP），工业屏蔽双绞线（ITP）以及光纤。TP 连接常用于端对端的连接。一个数据终端设备（DTE）直接连接到网络连接元件端口，而该设备负责将信号进行放大和转发。在 SIMATIC NET 工业以太网中，这些网络连接元件有 OLM（光学链接模板）ELM（电气连接模板）OSM（光学交换机模板）和 ESM（电气交换机模板）。DTE 与连接元件之间通过 TP 或 ITP 电缆连接。

1. 西门子以太网通信模块及集成有以太网接口的 PLC CPU

西门子大、中、小型机都提供有相应的以太网模块，都可用以使自身 PLC 接入以太网。有的 CPU 模块还集成有以太网接口，可直接接入以太网。同时，还有上位机使用的以太网接口卡以及相关以太网连接组件。完全使用西门子产品即可构建西门子的 PLC 以太网。

用于 PLC 主要的以太网模块有：用于 S7-200 的以太网模块 CP243-1、CP243-1 IT；用于 S7-300 的以太网模块 CP343-1、CP343-1 Lean 及 CP443-1；用于 S7-400 的以太网模块 CP444、443-1 IT 及 CP443-1 Advanced。

1）CP243-1、CP243-1 IT。使用它们可使 S7-200 与工业以太网连接。可支持速率为 10/100Mbit/s 速率及半或全双工通信。可使用 STEP 7-Micro/WIN 编程软件进行组态、远程编程和维修（程序下载和上载，状态）。可与其他 S7 控制器交换数据。可提供与 S7-OPC 的连接。CP243-1 既可以作为客户机（Client），也可以作为服务器（Server）。一个 CP243-1 可同时与最多 8 个以太网 S7 控制器通信，即建立 8 个 S7 连接。除此之外，还可以同时支持一个 STEP 7-Micro/WIN 的编程连接。一个客户端（Client）可以包含 1 ~ 32 个数据传输操作，一个读写操作最多可以传输 212 个字节。如果 CP243-1 作为服务器运行，每个读操作可以传送 222 个字节。

CP243-1 IT 除了具有 CP243-1 的功能外，还支持一些 IT 功能，如 FTP（文件传送）、E-mail、HTML 网页等。具有 8MB 存储器的 FTP 服务器。

2）CP343-1、CP343-1 Lean、CP343-1 IT。使用它们可使 S7-300 与工业以太网连接。

可支持速率为 10/100Mbit/s 速率及半或全双工通信。拥有一个预定的唯一以太网地址，通过网络可直接使用。具有自己的处理器，层 1 ~ 4 符合国际标准，可独立处理工业以太网上的数据拥塞；可 TCP/IP 和 UDP 等多协议运行；可为所有有源/无源通信伙伴的 TCP 传输连接。表 5-21 所示为这几个型号模块所支持的功能。

表 5-21　CP 343-1 等模块所支持功能

自动化系统		所支持的功能					
		PG/OP	S7	S5 兼容	ProfiNet		IT
					CBA	IO	
S7/C7-300	CP 343-1 Lean	●	●④	●	—	●①	—
	CP 343-1	●	●	●	●	●③	—
	CP 343-1 Advanced	●	●	●	●	●②	●
S7-400/S7400H	CP 443-1	●	●	●	—		—
	CP 443-1 IT	●	●	●	—		●
	CP443-1 Advanced	●	●	●	●	●②	●

① PROFINET IO 设备；

② PROFINET IO 控制器；

③ PROFINET IO 控制器或 PROFINET IO 设备；

④ 仅服务器。

2. ProfiNet 服务

与 PLC 网络有关的主要服务如图 5-64 所示的图解说明。其与 S7 系列 PLC 关系密接部分简述如下：

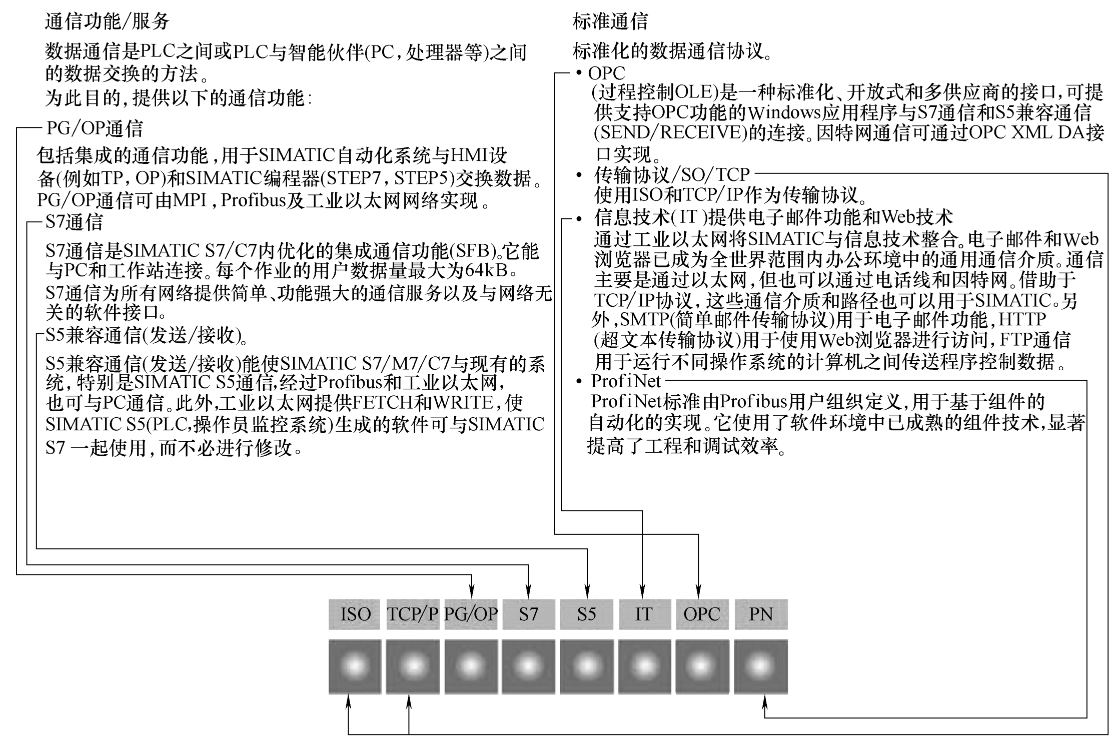


图 5-64　与 PLC 网络有关的主要服务图解说明

（1）PG/OP 通信服务

支持 S7 控制器与各种 HMI 设备或编程设备（编程设备/PC）通信的协议。典型的 HMI 设备有，操作员面板（OP）、触摸面板（TP）、多功能面板（MP）及文本显示（TD）。由于 S7 通信功能内置在 SIMATIC 控制器的操作系统中，所以可使用 HMI 设备、编程设备（PG）或 PC 来访问控制器中的数据。

（2）S7 通信服务

S7 通信服务使用通信系统功能块（SFB）和功能块（FB）为组态的 S7 连接提供数据交换功能。所有 SIMATIC S7 和 C7 控制器都集成了 S7 通信服务，通过这些服务使用户程序可以读取或写入数据。S7-400 控制器使用 SFB，而 S7-300 或 C7 控制器则使用 FB。这些功能与所使用的通信服务无关，允许通过 ProfiNet、工业以太网、Rrofibus 或 MPI 使用 S7 通信。S7 通信服务具体功能有：在系统组态期间，将组态 S7 通信要使用的连接；在下载新组态之前，一直可使用这些已组态的连接；可建立到同一通信伙伴的多个连接；可随时访问的通信伙伴数受限于 CPU 或 CP 上可用的连接资源数；S7 通信使您在每次调用 SFB 或 FB 时能传输最多 64KB 的数据块，S7-400 每次调用块时最多传输四个变量，S7-300 每次调用块时最多传输一个变量。

3. 集成有以太网模块的 PLC CPU

西门子 PLC CPU 类型、规格很多。集成有以太网模块的标准型 CPU 有：CPU 315-2 PN/DP、CPU 317-2 PN/DP 及 CPU 319-3 PN/DP。它们的 PN 接口是一个基于 Ethernet TCP/IP 的 ProiNet 接口。可支持：SIMATIC 控制器间进行数据的 S7 通信；用于通过 STEP 7 进行编程、调试和诊断的 PG/OP 通信；与 HMI 和 SCADA 连接的 PG/OP 通信；基于 ProfiNet 和 SIMATIC NET OPC 服务器的开放式 TCP/IP 通信；支持作为 ProfiNet I/O 控制器控制分布式 I/O；支持 ProfiNet CBA。

4. 计算机以太网卡

用于 PC/PG 的以太网网卡有 CP1616、CP1613、CP1612 及 CP1512 等。如 CP1616 通信处理器是 PCI 模块（插板），用于将计算机和 SIMATIC PG/PC 连接到 ProfiNetIO。CP 1616 的 ProfiNetIO 服务允许其用作 IO 控制器和/或 IO 设备。其最重要的功能如，已针对 ProfiNetIO 进行最优化集成式 4 端口实时交换机，可用于实现星型拓扑和总线拓扑支持的实时通信。支持同步实时通信。开发套件（用于在任何操作系统平台上集成 CP 1616）全面的诊断选项。

5. 从站模块

有通信接口及 I/O 模块。与控制器结合构成远程 PorfiNetI/O 系统。型号及规格都很多。有 ET 200pro、ET 200eco DP、ET 200M、ET 200s compact 及 ET 200eco PN 等。

ET 200pro 防护等级 IP65、IP66 及 IP67，最多可扩展 16 个模块，128 点或长度可达 1 米，支持 Profibus 以及 Profinet。应用环境更广泛，可应用于 −25℃ 的恶劣环境中。有可选择的总线与电源连接方式。

ET 200M 由以下部分组成：IM153 接口模块，用于与 Rrofibus-DP 或 ProfiNet 现场总线的连接。各种 I/O 模块，用总线连接器连接或插入在有源总线模块内。系统运行时可更换模块。

在 ET200S 分布式 I/O 家族中，增添有支持 ProfiNet 功能的 IM151-8 PN/DP CPU。其特点是：工作存储器容量 128KB，单位指令执行时间为 100ns；站点宽度可以达到 2m 或最大

可以扩展到63个模块；带有3个功能完全相同的ProfiNet接口，可以轻松实现线性拓扑结构；支持ProfiNet中的RT和IRT通信功能；作为ProfiNet I/O控制器，可以连接128个I/O设备；支持ProfiNet CBA功能；支持开放的以太网通信，包括TCP/IP，UDP，ISO-ON-TCP；集成网页服务器功能，可以轻松查询站点诊断信息，故障信息；可以通过以太网实现时钟同步功能（NTP）；通过扩展Rrofibus-DP主站接口模块，可以实现Rrofibus-DP主站功能；可以通过网络对Firmware进行更新等。

6. SIMATIC NET工业以太网网络部件

SIMATIC NET工业以太网网络部件包括工业以太网链路模板OLM，ELM和工业以太网交换机OSM/ESM和ELS以及工业以太网链路模块OMC。其中OLM（光链路模块）有3个ITP接口和两个BFOC接口。ITP接口可以连接3个终端设备和网段，BFOC接口可以连接二个光路设备（如OLM等），速度为10Mbit/s。ELM（电气链路模块）有3个ITP接口和一个AUI接口。通过AUI接口可以将网络设备连接到LAN上，速度为10Mbit/s。在普通OSM上，电气接口（TP/ITP）都是10/100Mbit/s自适应的且线序自适应。光纤接口为100Mbit/s全双工的BFOC接口，适用于多模光纤连接。二个OSM之间的最远距离为3km。在同一个网段上最多可以连接50个OSM，则扩展距离为150km。同时它还有地址学习、地址删除、设置传输波特率（10或100Mbit/s）及自适应功能，简化了网络配置和增强了网络扩展能力。此外，根据IEEE802.1Q标准，OSM/ESM还支持VLAN（虚拟局域网），它提供数据包的VLAN优先权标签。它将数据分配为由低到高（0~7）的优先权级别，对于没有目的地址的数据包则被视为低优先权的数据帧。

7. 交换机

按西门子的说法，交换机是以太网的核心。所以，交换机在组建以太网中是很重要的。西门子提供有不同功能的产品，有两种可用的交换机模型：封装在外壳中的外部交换机及集成在S7 CPU、S7 CP或分布式I/O系统ET 200中的集成交换机（例如在S7 CPU 41x-3PN中）。这也是西门子以太网接口模块的一大特点。但有的接口模块没有有带这集成交换机。带集成交换机的通常具有两个端口，用于网络的线性总线结构。有的还提供有3个或更多端口，可连接树型拓扑。图5-65所示为STEP 7中IO控制器和IO设备的ProfiNet接口的表示。

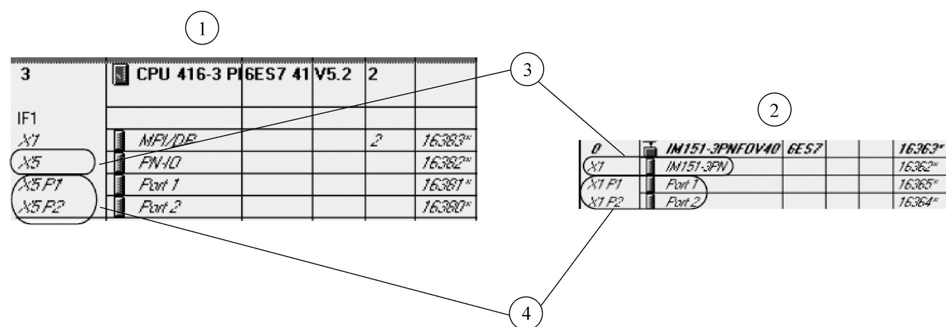


图5-65 ProfiNet接口表示

图中①为IO控制器的ProfiNet接口，②为IO设备的ProfiNet接口。③为该行表示ProfiNet接口的“接口”，④为这些行表示ProfiNet接口的“端口”。

外部交换机有入门型SCALANCE X-005、非网络管理型SCALANCE X-100、网络管理型

SCALANCE X-200、等时同步实时 SCALANCE X-200IRT、网管增强型 SCALANCE X-300 及高性能模块化 SCALANCE X-400 等。分别可满足不同的组网需要。

入门型工业以太网入门级交换机，配有 5 个传输速率可达 10/100Mbit/s 的 RJ45 端口。

非网管型交换机有电气和电气/光学两种可用形式，可实现电气电路和光学电路的相互转换。价格低廉，可构建具有交换功能的小型星形结构或线形结构。型号不同性能也不同。如 SCALANCE X12 4 可配置 24 个电气端口。最适合用于总线型和星形型网络结构组态（10/100Mbit/s）。再如 SCALANCE X106-1 可配置 6 个电气端口和一个光学端口（BFOC）。

网管型交换机最适合用于总线型和星形结构（10/100Mbit/s）的以太网。可作为冗余管理器与 SCALANCE X-400/X-200IRT 或 OSM/ESM 组合，实现了环形冗余，提供网络的可靠性。也有电气和电气/光学两种形式及多种型号。型号不同性能也不同。如 SCALANCE X224 可配置 24 个电气端口。再如 SCALANCE X206-1/X206-1 LD 可配置 6 个电气端口和一个光学端口（BFOC）。

等时同步实时 SCALANCE X-200IRT 交换机可用于配置实时和同步实时网络，以进行大量的实时数据和标准数据通信（TCP/IP）。可组建环形冗余结构和两个子网，例如，通过 SCALANCE X-200IRT 交换机可连接冗余的环形网。也有有电气和电气/光学两种形式及多种型号。型号不同性能也不同。如 SCALANCE X204IRT 可配置 4 个电气端口。再如 SCALANCE X202-2IRT/X202-2P IRT 可配置两个电气端口和两个光学端口（BFOC 或 POF/PCF）。

网管增强型交换机适用于组建总线和星形结构（10/100Mbit/s）的以太网。交换机之间可以建立千兆以太网连接。双绞线用户可以直接连接设备。SCALANCE X-400 交换机可与之配合，例如，处理诸如 PCS7 控制系统。可存在以下的网络拓扑和拓扑的组合：高速以太网和具有高速媒介冗余的千兆级以太环网；为了防止传输链路或者交换机发生错误，多达 50 个 SCALANCE X-300 交换机流线型排列连接到一个环状网内，对于双模的可组成一个总共长达 150km 的线路，或者对单模可组成一个总共长达 1300km 的线路。当环状网内一个传输路径或者 SCALANCE X-300 交换机发生错误，传输路径可在 0.3s 内重构。采用 SCALANCE X-300 交换机的星形结构：每个 SCALANCE X-300 交换机有一个星形触点可通过电信号或者光信号与多达 26 个节点或子网相连。用来连接双绞线的数据端子，或者网段（10/100/1000Mbit/s 级）。也有电气和电气/光学两种形式及多种型号。型号不同性能也不同。如 SCALANCE X310 带有 3 个千兆级端口和 7 个高速以太网端口的交换机。再如 SCALANCE X308-2LD 带有 1 个千兆级电气端口、7 个高速以太网端口和 2 个千兆级单模玻璃纤维光学端口（含有 SC 插座）的交换机。

高性能模块化交换机性能更高。适合于组建为高性能的线型，星形和环状结构（10/100/1000Mbit/s）的工业以太网络。用在过程控制系统（例如 PCS 7）中。

5.5.3 西门子 PLC 以太网配置实例

1. 计算机通过以太网与 S7-200 PLC 联网组态实例

（1）局域网连接

其配置如图 5-66 所示，计算机用以太网接口，通过以太网与两台分别配置有以太网（CP 243-1）模块和互联网（CP 243-1IT）模块的 S7-200 连网。

连网后，计算机运行 STEP 7-Micro/WIN 编程软件，可监控 PLC，上下载 PLC 程序、设置及相关数据。同时，安装了 STEP 7-Micro/WIN 之后，计算机上会有一个标准浏览器（S7-

200 Explorer)，可用它来访问互联网（CP 243-1 IT）模块的主页。如果计算机可运行其他有关应用程序，也可监控 PLC，或与 PLC 交换数据。同时，PLC 之间也可通信、交换数据。而为实现这些功能还须做以下 3 方面的组态：

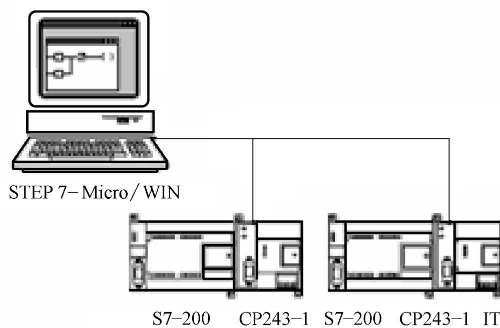


图 5-66　10/100 兆以太网

1）计算机方组态。计算机需配置使用 TCP/IP 协议。具体应在设置 PG/PC 接口对话框中，选取对应的以太网接口协议。当安装好西门子编程软件后，此设置接口会自动加载在 Windows 的“我的电脑”的“控制面板”中。运行 STEP 7-Micro/WIN 编程软件后出现的“View”中也有该窗口。只要点击“控制面板”或“View”中该项，即可弹出此窗口。

2）CP-243-1 组态。可点击 STEP 7-Micro/WIN 编程软件的主菜单“Tools”下“Ethernet Wizard”（以太网配置向导）项，在弹出“Ethernet Wizard”窗口后，按提示一步步操作。主要是对模块的 IP 地址，使用的内存区做指定。在完成以太网向导后，会生成一个网络配置子程序（ETHx_CTRL）。如图 5-67 所示，要在程序中用 SM0.0（常 ON 接点）调用这个子程序。该图中的状态字 VW0、VW2 地址由用户指定，要注意不能与其他做配置时指定的 V 存储区重复。

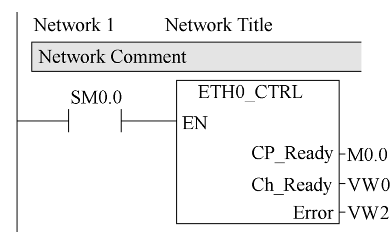


图 5-67　以太网控制子程序

将此程序下装到 CPU 中，然后将 CPU 重新上电，并运行，此时对以太网的配置才开始生效。结合上述完成的计算机上设置 PG/PC 接口组态，即可进入 Communications（通信）中与 CPU 编程通信。

如果要进行 S7-200 PLC 之间通信，还须在以太网配置向导中指定连接数（细节见下例）。最多可组态 8 个连接。每个连接可以是服务端，也可是客户端。前者用以接受对方访问（可以是指定一个对方，也可多个），后者用以访问对方。如果组态为客户端，还要指定对方 IP 地址，传送（读写）的数据区，组态完成后会生成数据传送子程序（ETHx_XFR）；如果组态为服务端，可选定一个（要指定与其连接的 IP 地址）或多个连接。组态完成后生成子程序。有了这子程序，PLC 间要通信，可由客户端执行器生成的子程序，发起通信，服务端不必运行程序即可响应。进而实现双方交换数据。

要指出的是，其他厂家的 PLC 虽也支持以太网 TCP/IP 协议，但不能与西门子的 CPU 用以太网通信。因为在应用层协议中，西门子使用的是 S7 协议。其他厂家的 CPU 虽然能接收到西门子 CPU 的数据包，却读不懂 S7 协议的内容，反之亦然。西门子的以太网模块只允许在西门子的产品间进行工业以太网通信。再 CP243-1 上只有一个 RJ45 口，没有 BFOC 口，不能与光纤电缆直接连接。但可以用一个 OMC（单点）模块或 OSM（多点）模块来将 RJ45 口的连接转换成光纤连接。通过无线交换机等网络设备，CP243-1 可以连接无线以太网。

3）CP-243-IT 组态。除了要进行如 CP-243-1 一样的以太网组态之外，还要进行 IT 组态。不管哪个组态都使用 STEP 7-Micro/WIN 编程软件的主菜单“Tools”下“Internet Wiz-

ard”（互联网配置向导）项，在弹出“Internet Wizard”窗口后，按提示一步步操作。除了与 CP243-1 一样做好以太网组态。还要选择是否进一步做 IT 组态。如果要组态所有 IT 功能，则生成 ETHx_EMAIL、ETHx_FTPC 子程序。可分别调用以向对方发送电子邮件及进行 FTP 文件传送。至于 WEB 服务，连网后在计算机上用浏览器键入其 IP 地址即可进入页面，即它的起始页面。进而可点击有关链接进入其他页面。西门子供应 CP243-IT 模块时还提供可用 Java 语言编辑页面的工具。这些属于编程的范围。这里略。

（2）互联网连接

如图 5-68 所示，计算机还可通过互联网与 PLC 连接。

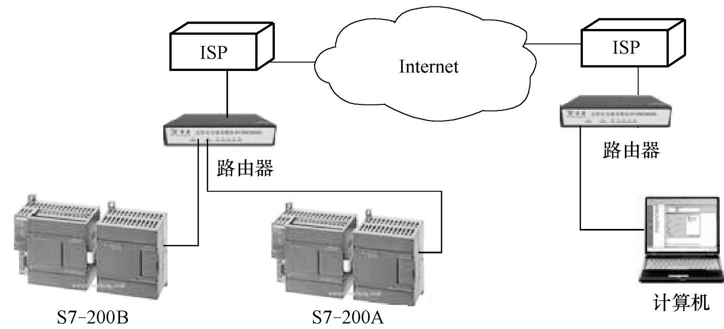


图 5-68　计算机通过互联网与 PLC 联网

从图知，这里 PLC 站点与计算机站点都是通过路由器、ISP（Internet Service Provider，互联网服务供应商服务器）接入互联网。然后进行通信。

为了 PLC 系统安全，建议在 PLC 方最好使用可设定密码的路由器，如图 5-69 所示的深圳赛远公司的 SY-RSCM300。其主要性能有：全双工 10/100Mbit/s；路由及防火墙功能；可设置密码；工业 IC 设计稳定可靠；支持广域网、局域网等。该公司同时还提供有设置与使用软件。



图 5-69　深圳赛远公司 SY-RSCM300

从图知，它除了外接电源，还有配置口（用于路由器以配置）、一个 WLAN 口（上接互联网接）及 4 个 LAN 口（可接 4 个 PLC）。为了使用该产品，该公司还设有测试实验系统，提供有 SY-RSC 远程通信接入软件、账户与密码。运行此软件后出现的界面如图 5-70 所示。

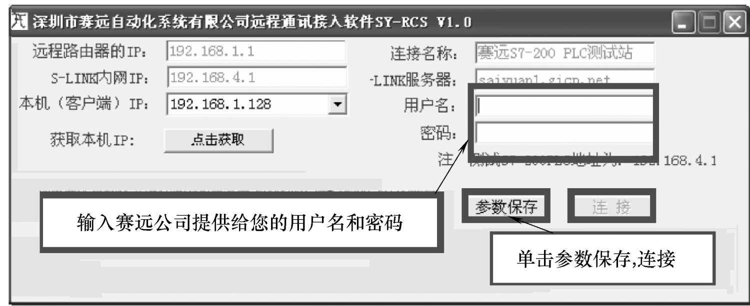


图 5-70　远程接入软件界面

从图知，只要输入所提供的账户、密码，先点击【参数保存】键，后点击【连接】键。单击完以后耐心等待，依据计算机和网络的速度，一般连接服务器时间为 30 ~ 60s 左右。如账号、密码正确，网络正常将弹出连接成功的应答窗口。并在计算机桌面右下角出现网络连接小图标。计算机还增加一个与上述账号、密码对应连接。

连接成功后，打开 S7-200 编程软件 STEP 7 MicroWIN V4.0 SP7。先按图 5-71 所示操作，设置 PG/PC 接口。



图 5-71　设置 PG/PC 接口

进而按图 5-72 所示配置 S7-200IP 地址。

在配置正确的 IP 地址，并刷新后，如果如图 5-73 所示，显示该 IP 地址，表示连接到了远程的 PLC。

一旦连接成功，如同当地串口与 PLC 连接一样，可上下载程序、数据，对 PLC 监控。可完成运行编程软件所有的工作。

2. S7-200 PLC 通过以太网与 S7-300 PLC 联网实例

先组态 S7-200，后组态 S7-300。

（1）S7-200 组态

其步骤是：

1）打开以太网向导。用 STEP 7-Micro/WIN 编程软件的主菜单“Tools”下“Internet Wizard”向导。只是在组态连接时，要如图 5-74 所示，建立 1 个连接。

2）组态连接。在该图 1 处填写模块占用的输出地址，建议使用默认值。2 处配置模块的连接个数，最多可 8 个，本例为 1。最后在 3 处点击“Next”按钮，将弹出如图 5-75 所示的“Configue Configurations”（连接组态）窗口。

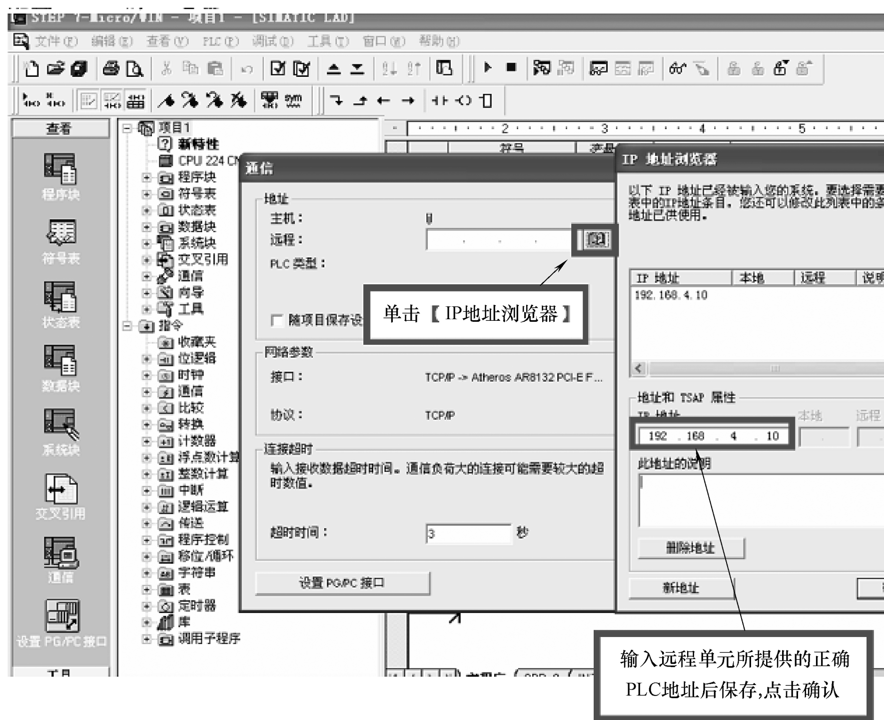


图 5-72 配置 S7-200IP 地址



图 5-73 显示 IP 地址连接成功

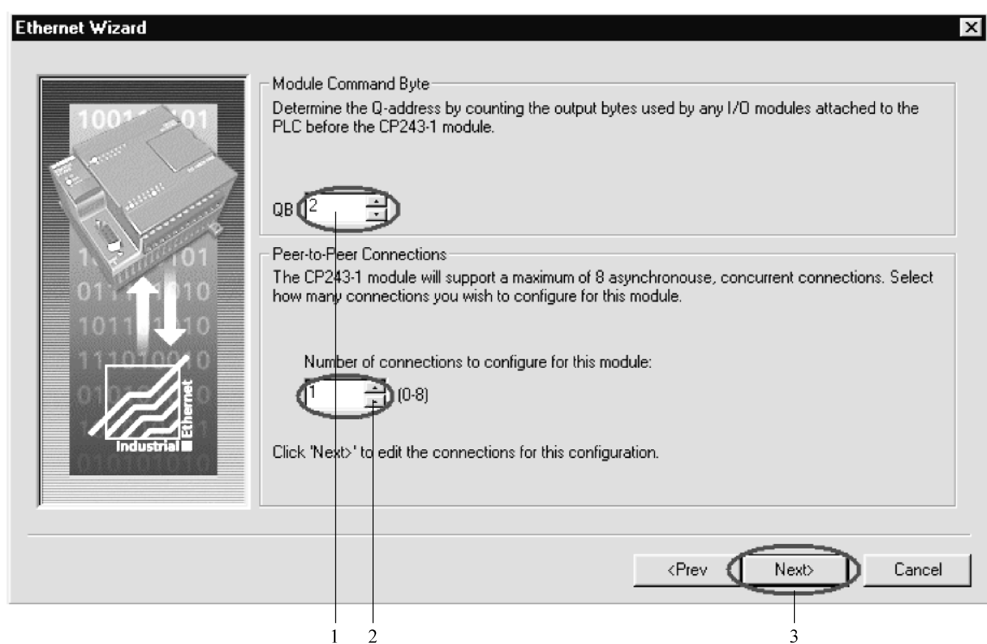


图 5-74　建立 1 个连接

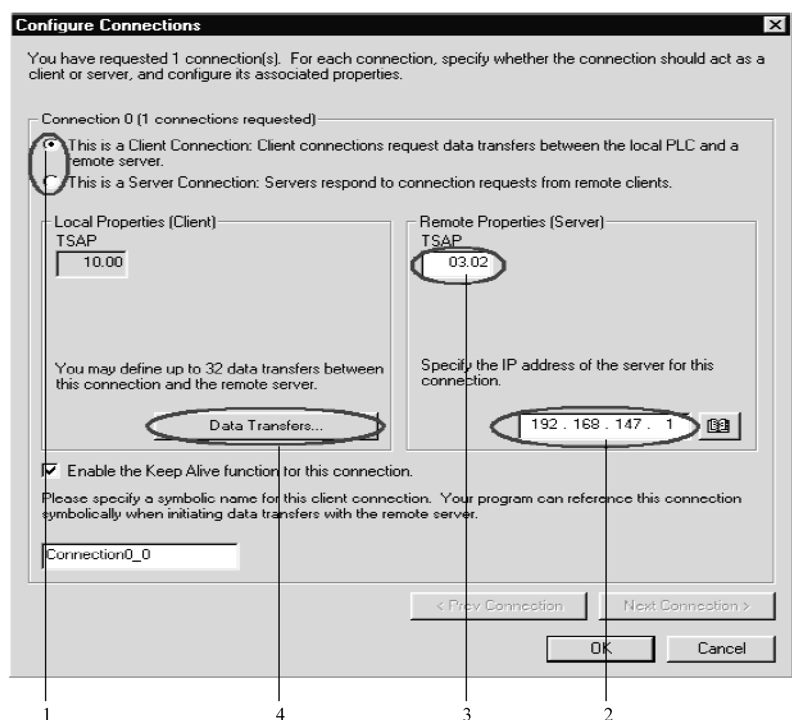


图 5-75　Configue Configurations 窗口

3）组态客户端。在该窗口 1 处配置该模块为 CLIENT。在 2 处填写 SERVER 端的 IP 地址。在 3 处填写 TSAP（传输服务访问点）地址，请使用 03.02。如果进行了联网，两个站的节点地址（MAC 或 IP 地址）已经确定。两个连接端上的本地/远程 TSAP 或端口会自动获得默认值。最后在 4 处点击“Data Transfers”按钮，将弹出如图 5-76 所示“Configue CPU-to-CPU Data Transters”（CPU 到 CPU 传送组态）窗口。

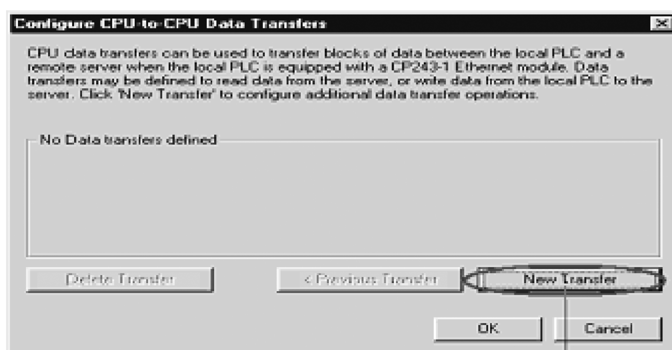


图 5-76　Configue CPU-to-CPU Data Transters 窗口

4）进入参数组态画面。这时该窗口还空的，还没有定义数据传送。为此可点击“New Transfer”按钮，可进入如图 5-77 所示参数组态画面。

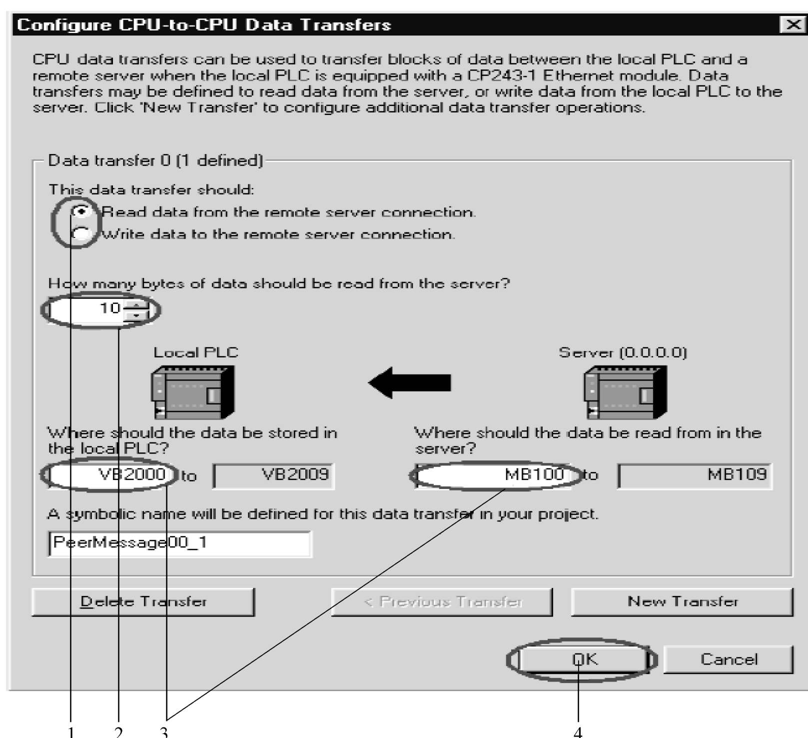


图 5-77　参数组态画面

5）确定读写数据地址。在该窗口 1 处选择是读取数据还是写入数据。2 处填写通信数据的字节个数。3 处填写发送数据区和接收数据区的起始地址。之后，在 4 处点击“OK”

按钮，将回到如图 5-74 所示“Configue Configurations”（连接组态）窗口，并在其上点击“OK”按钮，将弹出如图 5-78 所示校验组态画面。

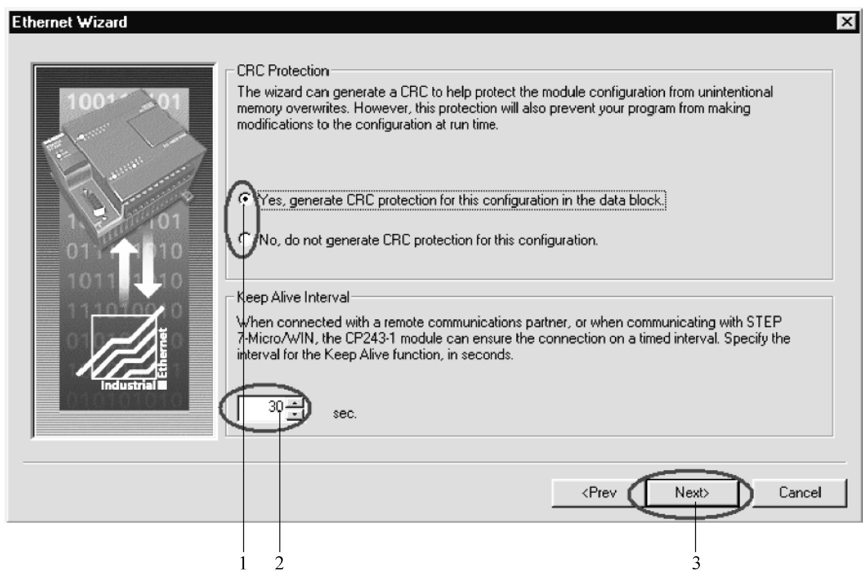


图 5-78　校验组态画面

6）确定 CRC 校验。在该窗口 1 处选择 CRC 校验。2 处使用缺省的时间间隔 30s。最后点击“Next”按钮，将弹出如图 5-79 所示分配内存地址窗口。

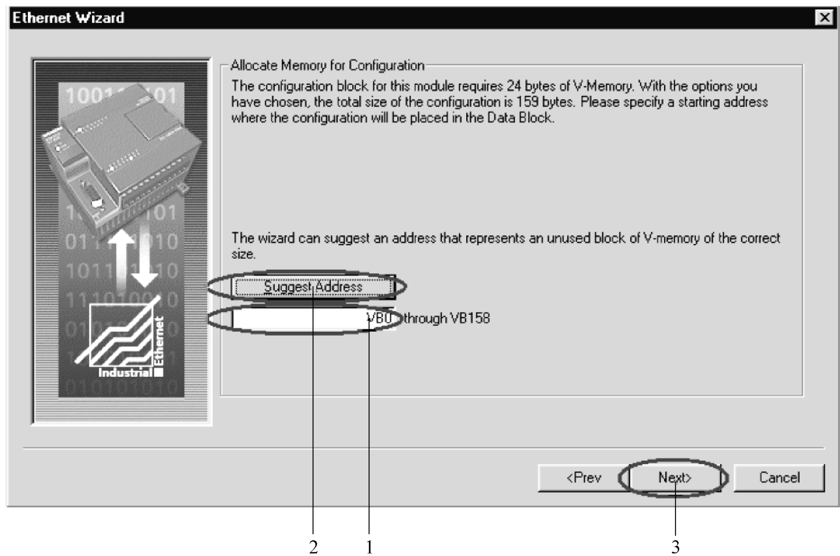


图 5-79　分配内存地址窗口

7）确定占用 V 存储区地址。在该窗口 1 处填写模块所占用的 V 存储区的起始地址。2 处可通过 Suggest Address 按钮获得系统建议的 V 存储区的起始地址。最后点击 3 处“Next”按钮，将弹出如图 5-80 所示组态完成窗口。

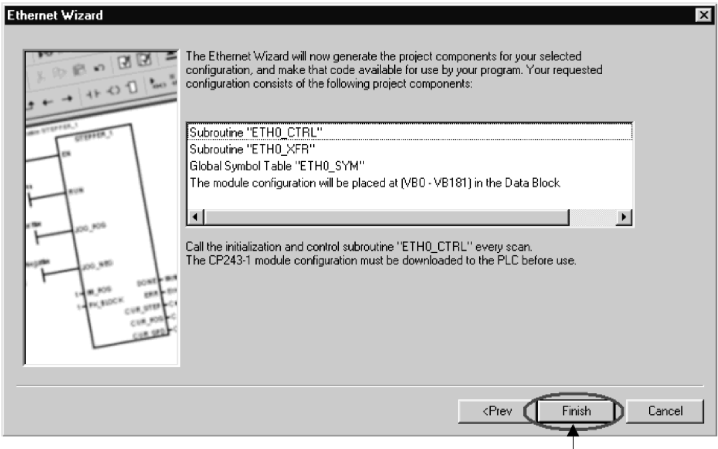


图 5-80　组态完成窗口

8）生成子程序及数据块。可在其上点击“Finish”按钮，即完成对该模块的组态。从图 4-7 可知，这时生成了 2 个子程序及 1 个数据块。可用以模块的初始化及数据读写调用。

9）编写子程序调用程序。具体程序如图 5-81 所示。用它可激活以太网模块。同时可从所组态连接的服务器指定区读取数据，并存于上述组态的内存区中。

当然，也可把 S7-200 组态为服务器。这时就对方运行程序，读取本站的数据。具体组态略。

（2）组态 S7-300

要使用 STEP 7 编程软件。其步骤如下：

1）打开软件后，先建立新工程，组态 S7-300 站点。并点击“Options”菜单项下的“Configure Network”项，进入如图 5-82 所示的“NetPro”窗口。

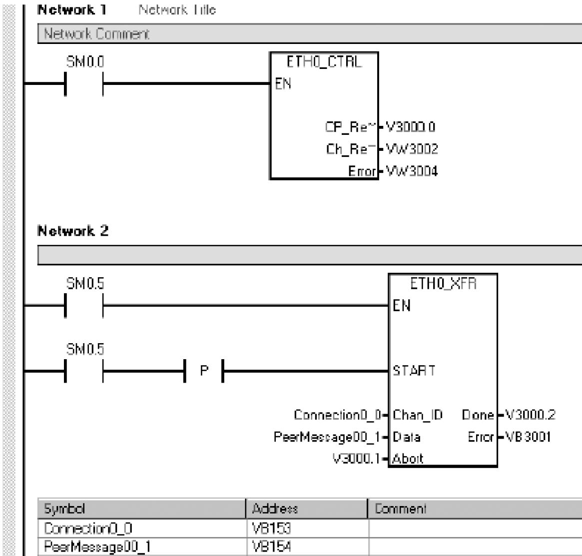


图 5-81　组态完成窗口

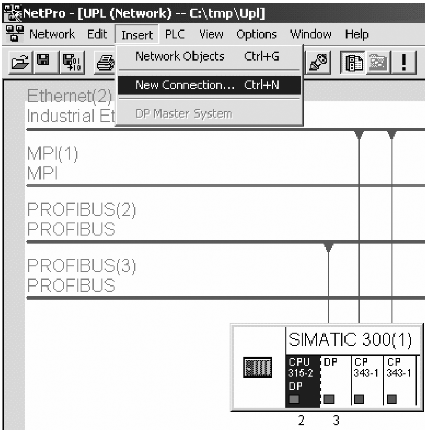


图 5-82　NetPro 窗口

2）点击 S7-300 站（如图示呈深色），再点击“Insert”菜单项的“ New Connection...”项，将弹出如图 5-83 所示的“Insert New Connection”窗口。

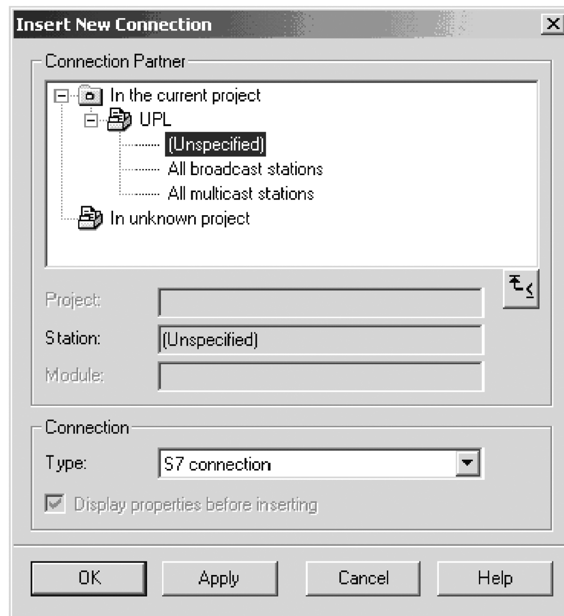


图 5-83　Insert New Connection 窗口

3）选择连接类型。本例选择“unspecified S7 connection”。并点击“OK”按钮。之后将弹出如图 5-84 所示的“Properties of the S7 connection”窗口。

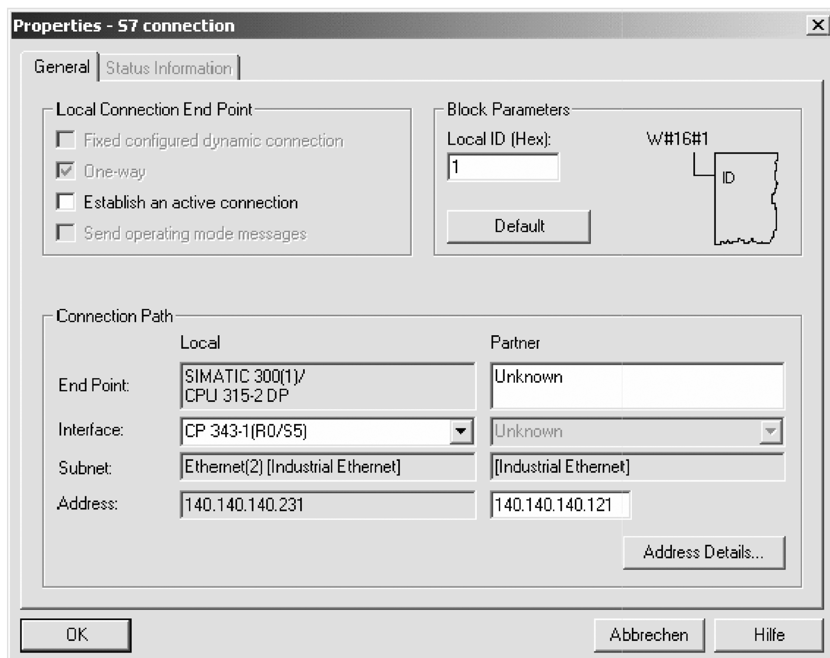


图 5-84　Properties of the S7 connection 窗口

4）激活连接。因这时 S7-200 已组态、连网，并拥有 IP 地址。故在标记“Establish an active connection”项，输入 S7-200 的 IP 地址，并点击“Address Details...”按钮，将弹出如图 5-85 所示的“address details”窗口。

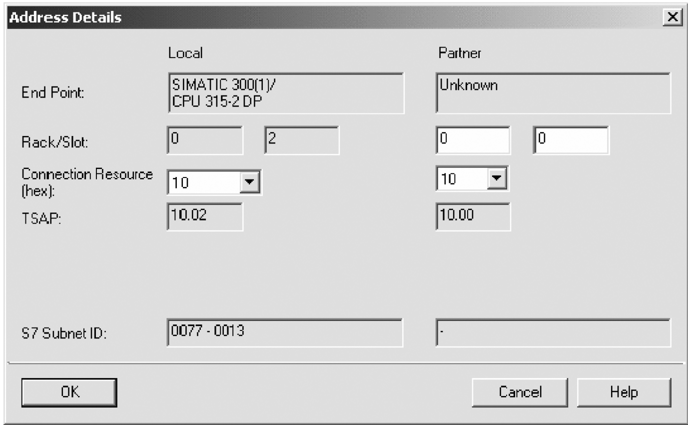


图 5-85 address details 窗口

5）确定 TSAP。对方（Partner）组态应与 S7-200 当初的相同。而当地（S7-300）的组态应为 10 + Connection 号 . 机架号 + CPU 槽号。本例为 10. 02。

6）编辑并存储。然后由“NetPro”下载给 S7-300 站。

7）建立数据块 DB11，其长度要足够长，以便于交换数据，也下载此数据块给 S7-300。至此组态完成。

8）这时，只要 PLC 在线运行、网络工作，打开“STEP 7 Micro/WIN”软件，在线后，通过状态表，即可监视到接收到存放 VB1000 中的数据。

3. 两套 S7-300 通过以太网实现通信组态实例

首先搭建一套测试设备，设备的结构图如下：两套 S7-300 系统由 PS307 电源、CPU314C-2DP、CPU314C-2PTP、CP343-1、CP343-1 IT、PC、CP5611、STEP7 组成。具体组态步骤如下：

1）打开 SIMATIC Manager，根据我们系统的硬件组成，插入两个 S7-300 的站，插入 CPU，并开始相应硬件组态。

2）分别插入两个系统的以太网模块。如图 5-86 所示在 CPU 314C-PtP 机架上插入 CP343-1 模块。在弹出的“Properties-CP343-1”窗口上，点击“Properties”按钮。

3）之后将弹出如图 5-87 所示的“Properties-Ethernet interface CP343-1 ”窗口。并在其上设置 IP 地址及子网掩码，并建立以太网。

4）另一 S7-300 站也做类似组态。组态完两套系统的硬件模块后，分别进行下载，然后点击 Network Configration 按钮，打开如图 5-88 所示的系统的网络组态窗口 NetPro，并选中 CPU314。

5）在窗口的左下部分点击鼠标右键，插入一个新的网络链接，并设定链接类型为 ISO-on-TCP connection 或 TCP connection 或 UDP connection 或 ISO Transport connection，如图 5-89 所示。

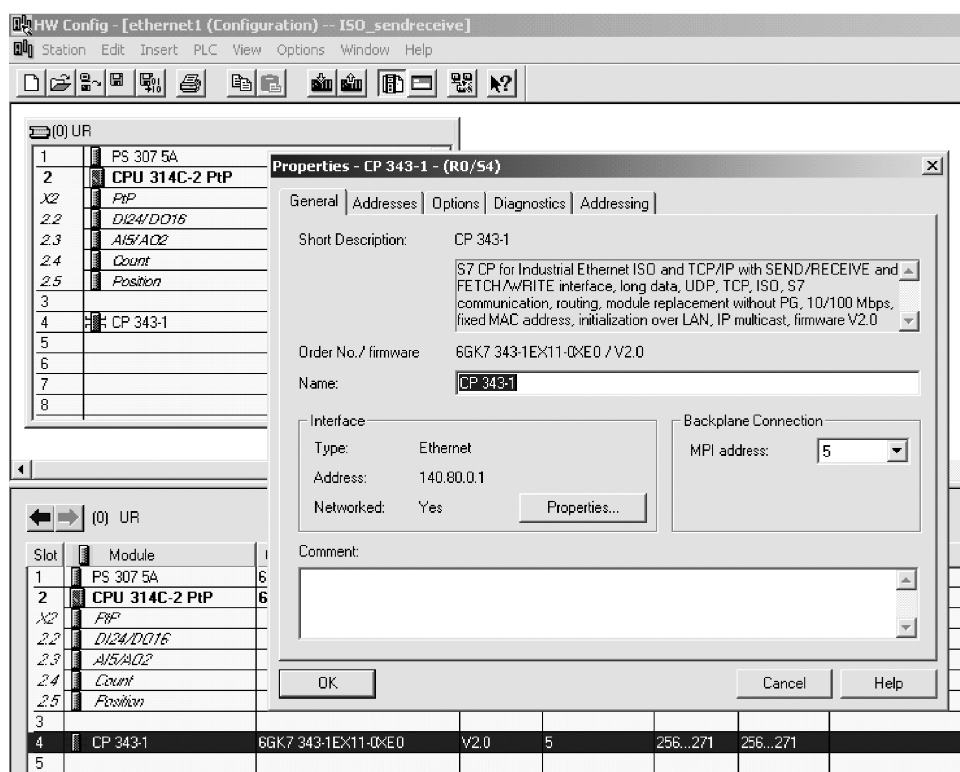


图 5-86　插入 CP343-1 模块

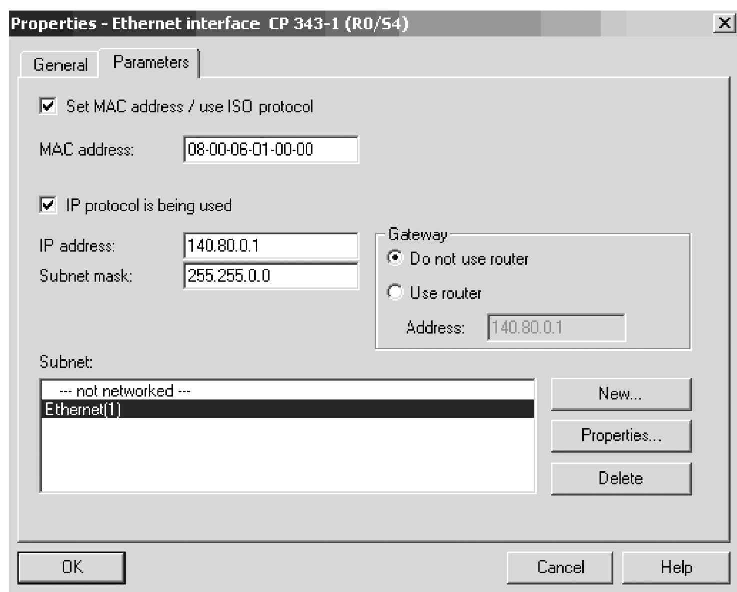
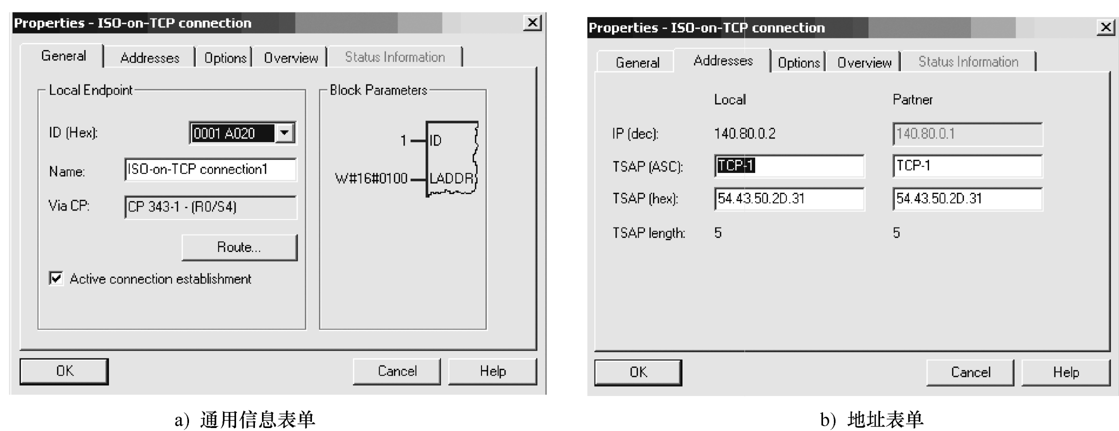


图 5-87　Properties-Ethernet interface CP343-1 窗口

图 5-88 网络组态窗口上选中 CPU314

图 5-89 插入新连接

6）以上选定后，点击“OK”按钮，将弹出如图 5-90 所示“Properties-ISO-on-TCP connection”（链接属性）窗口。使用该窗口的默认值，并根据图 5-89 对话框右侧信息再进行有关程序块的参数设定。



a) 通用信息表单　　　　b) 地址表单

图 5-90　Properties-ISO-on-TCP Connection 窗口

7）当两套系统之间的链接建立完成后，用鼠标选中图标中的 CPU，分别进行下载。

8）到此为止，系统的硬件组态和网络配置已经完成。下面进行系统的程序编制，在 SIMATIC Manager 界面中，分别在 CPU 314C-2PTP、CPU 314C-2DP 中插入 OB35 定时中断程序块和数据块 DB1、DB2，并在两个 OB35 中调用 FC5（AG_Send）和 FC6（AG_Recv）程序块，如图 5-91 所示。

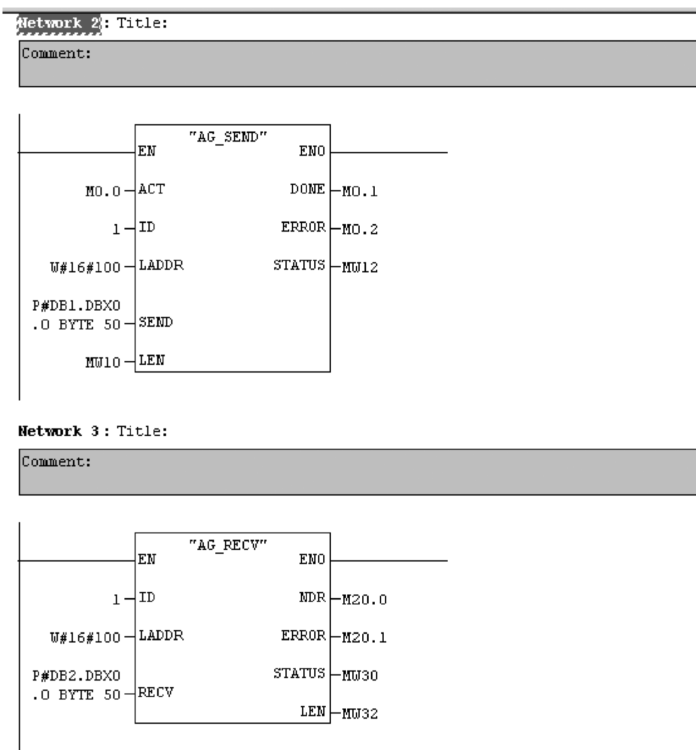
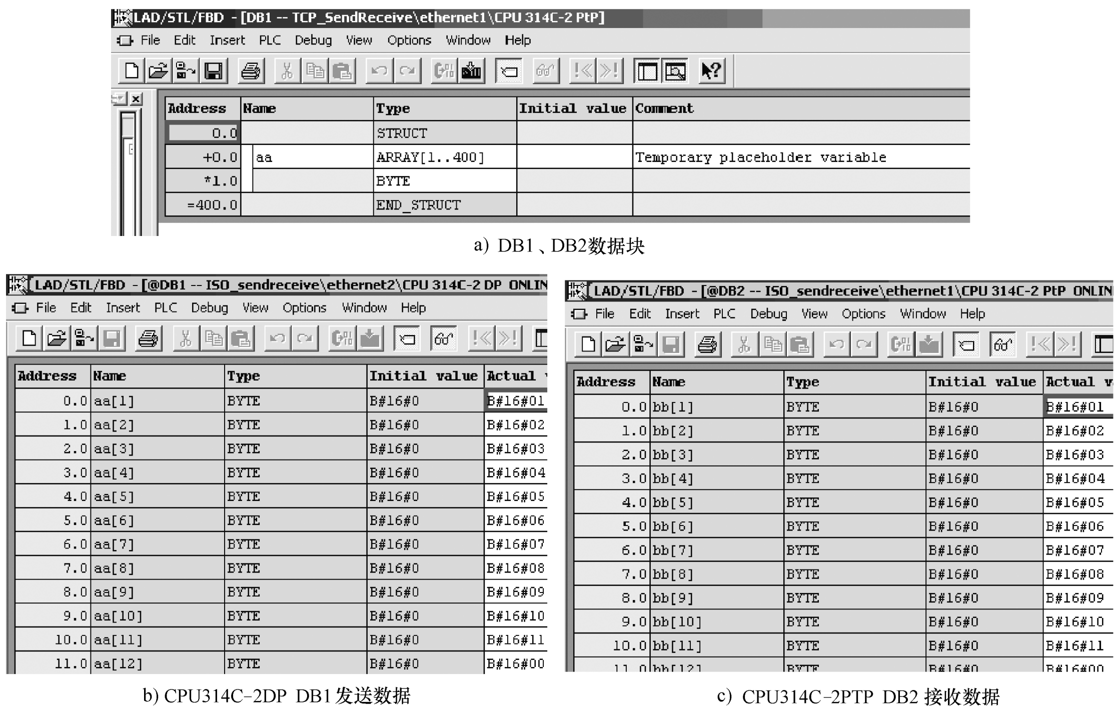


图 5-91　调用 FC5（AG_Send）、FC6（AG_Recv）程序块

9）创建 DB1、DB2 数据块，如图 5-92a 所示。

10）两套控制程序已经编制完成，分别下载到 CPU 当中，将 CPU 状态切换至运行状

态，就可以实现 S7-300 之间的以太网数据交换了。这点击编程窗口的“View”菜单项的“Data View”项，切换到数据监视状态，在图 5-93 所示的窗口上观测。从站可看到 CPU314C-2DP 的 DB1 数据发送到 CPU314C-2PtP 的 DB2 情况。



a) DB1、DB2数据块

b) CPU314C-2DP DB1 发送数据

c) CPU314C-2PTP DB2 接收数据

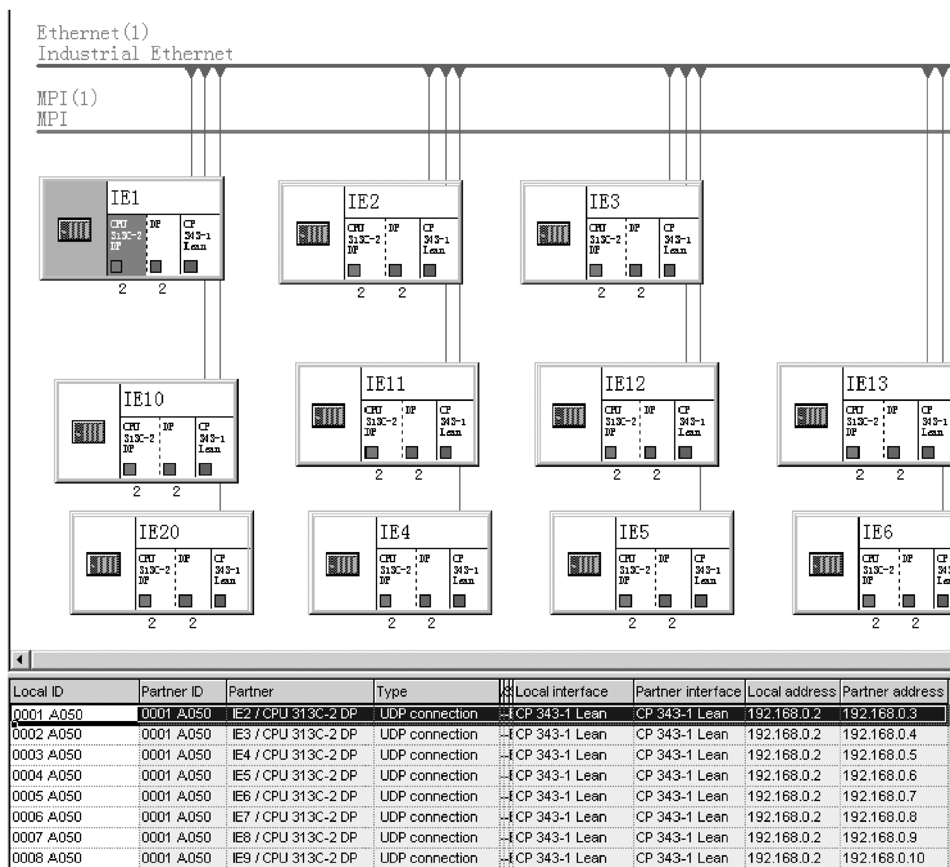
图 5-92 CPU314C-2DP DB1 及 CPU314C-2PtPDB2 数据块及其监视画面

除了上述两套连接，也可多套连接。一个实例就是沈阳旭风电子公司为本溪钢厂辽宁冶金技师学院所配置的 S7-300 实验室。该系统有 20 个实验台。每台都配置有 S7-300 及其以太网模块。同时还都配置计算机及以太网卡。这 40 个以太网接口都通过交换机连接，组成星形拓扑的因特网。20 台计算机、PLC 站点都有自身唯一的 IP 地址。如图 5-93 所示，每台 PLC 站点还分别命名为 IE1 ~ IE20（但该图仅显示部分站点）。

该图点击了 IE1 站点的 CPU 图标，从图下方可见到这里以组态的连接。指明了连接的类型是 UDP connection，自身及连接对方的 IP 地址。当然为了 PLC 间交换数据，连接双方的 PLC 还都得与上述 S7-200PLC 通过以太网与 S7-300 连网实例一样，定义数据块、编写相应程序调用 FC5、FC6 功能块。而网络上的任何计算机，如运行 Step 7 软件则可与网络上的任何一台 PLC 联机编程、监控。当然计算机间做好设置相互访问也是可以的。由于这里是实验室，用的是普通交换机，网络的实时性、确定性不是很理想。但作为实验、熟悉以太网组态及编程应用还是很理想的。再就是这里站点间建立连接的数量是有限制的。具体与因特网模块的性能有关。

4. PN CP IO 组态实例

本例用于 S7-300 通过工业以太网实现远程控制。本例使用的 CP 以太网模块是 CP343-1 Advanced-IT。因为它具有 Profinet IO 功能。其组态过程是：



Local ID	Partner ID	Partner	Type	Local interface	Partner interface	Local address	Partner address
0001 A050	0001 A050	IE2 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.3
0002 A050	0001 A050	IE3 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.4
0003 A050	0001 A050	IE4 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.5
0004 A050	0001 A050	IE5 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.6
0005 A050	0001 A050	IE6 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.7
0006 A050	0001 A050	IE7 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.8
0007 A050	0001 A050	IE8 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.9
0008 A050	0001 A050	IE9 / CPU 313C-2 DP	UDP connection	CP 343-1 Lean	CP 343-1 Lean	192.168.0.2	192.168.0.10

图 5-93　多套以太网连接实例

1）运行 S7 Step 软件，建立新工程。如图 5-94 所示，组态 S7-300 站点，添加 CP343-1 Advanced-IT 模块作为 IO 控制器，并建立空白 EtherNet［2］网络。

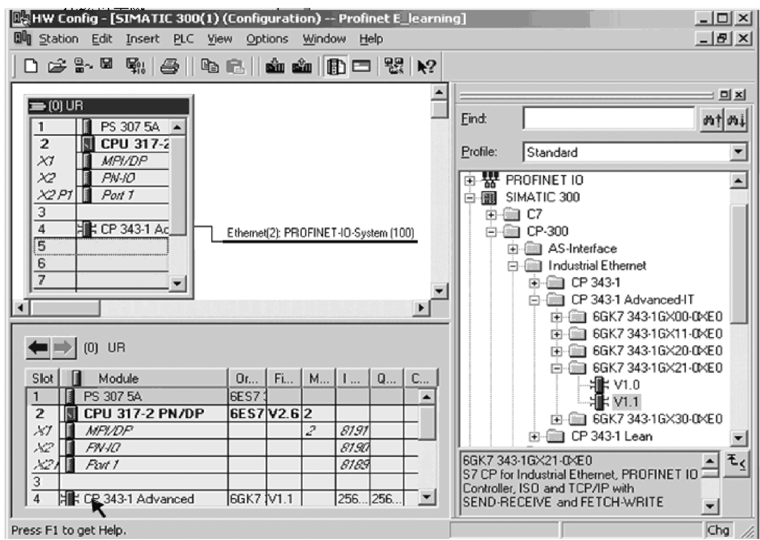


图 5-94　组态 S7 300 站点及建立 EtherNet［2］网络

2）图 5-94 所示的“NetPro”窗口添加两个 ET200S IO 设备站。办法如前例介绍，也是用鼠标拖放。如图 5-95 所示。

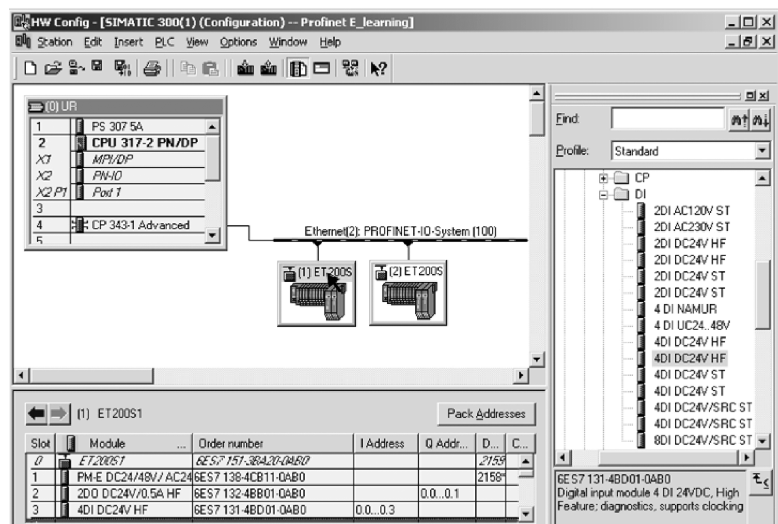


图 5-95 添加两个 ET200S IO 设备站

从图可看到，这里已组态了两个 ET300S IO 设备站。其接口都是用了 IM152-3PN。同时，也可看出［1］ET200S 站还添加好了电源及 DO、DI 模块。

3）编辑 IM152-3PN 属性。办法是分别双击上图［1］ET200S 站图标，将弹出如图 5-96 所示的 IM152-3PN 属性窗口。

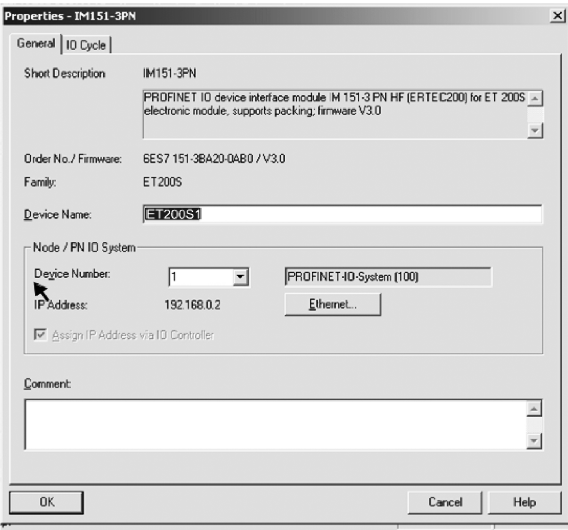


图 5-96 IM152-3PN 属性窗口

从中可看到 IP 地址，及可进行部件号及名称指定。本例指定号为 1，名称为 ET200S1。此名称很重要。在进一步在线组态时，要指派给 IO 设备站。

4）名称派给 IO 设备站。首先使计算机连网。之后在硬件组态窗口上，点击的“PLC”主菜单下的“Ethernet”项下“Assign”子项。将弹出如图 5-97 所示的“Assign device name”窗口。

从图看到有两个 MAC 地址的 IO 设备站。都是 ET200S，但没有 IP 地址及设备名称。为此要先指派与实际 MAC 地址相一致的名称。办法如图 5-98 所示，先点击要指派的 MAC 地址 IO 设备站，再在窗口左上方的部件名称栏中选择要指派的名称，然后用鼠标点击“Assign name”按钮。该图已对［1］站点指派了名称，正指派［2］站点。

完成所有站点指派，可点击其上“Close”按钮。窗口关闭。为了检查是否指派正正确，

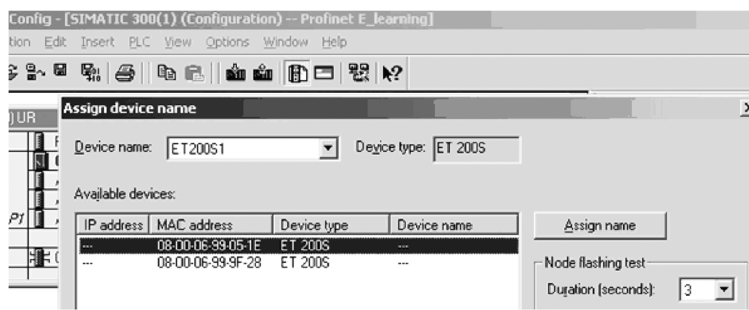


图 5-97　“Assign device name” 窗口

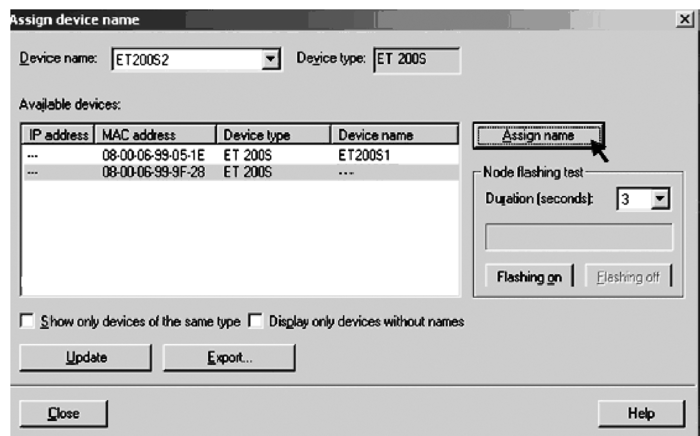


图 5-98　指派对应 MAC 地址的设备名称

可在硬件组态窗口上，点击的“PLC” 主菜单下的“Ethernet” 项下“Verify Device name” 子项。点击后将弹出如图 5-99 所示“Verify Device name” 窗口。

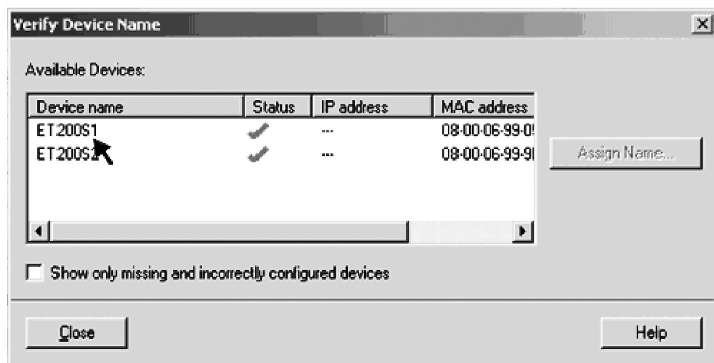


图 5-99　Verify Device name 窗口

从该图知，在它的 States 项下两个站点都打了“沟号”。说明名称指派正确，意味着硬件组态完成，可关闭该窗口。接下来要进行通信还要编程。这是因为，Profinet 处理这里的远程 IO 与当地的不同，要用建立数据块及调用功能函数 FC11（发送数据）、FC12（接收数

据)，把读的存于数据块中，要写的数据要从数据块中取。这点与 Ethernet/IP 或 Profibus DP 相比似乎稍有有不便，后两者完成组态后就有对应处理远程 IO 的地址，直接可在程序中使用。它的有关用程序读写数据块的细节牵涉到通信编程，这里就不再进一步讨论了。

5.6　三菱 PLC 以太网配置

关键词：主站、从站、基于以太网、循环通信、循时通信

三菱 PLC 以太网有传统的以太网及开放的 CC-Link/IE 以太网。本节主要介绍 CC-Link/IE 以太网。

5.6.1　CC-Link/IE 简介

CC-Link IE 继承了 CC-Link 循环通信技术，基于以太网，是从控制层网络到现场和运动控制网络的整合。也称为 CC-Link IE 整合网络，利用它可实现无网络层次的无缝数据传送。

1. CC-Link/IE 以太网组成

CC-Link IE 开发于 2007 年，原是基于光纤的千兆控制以太网。新开发的还有双绞线的千兆现场以太网。

(1) 千兆控制以太网 (Control)

有单层网络及多层网络，其组成如图 5-100 所示。

从图知，无论单层还是多层网络，特点是总要有一个，也只有一个管理（控制）站。其他的为普通站。多层网络只是有一个站点既是上一层的普通站，又是本层网络的管理站。管理站一般为 PLC 或计算机，而普通站除了 PLC、计算机，还可是人机界面、机器人等设备。管理站管理网络，如网络站点数、网络共享内存等确认与分配，以确保网络的完整性与一致性。普通站则要接受网络站管理。单层网络站点可多到 120 个。多层网络与三菱的传统控制网类似，也是一个个网络套接而成，最多可连接 239 个网络。各个网络要设定唯一的网络号。各站点也要设定其所在的网络号及唯一的站点号。

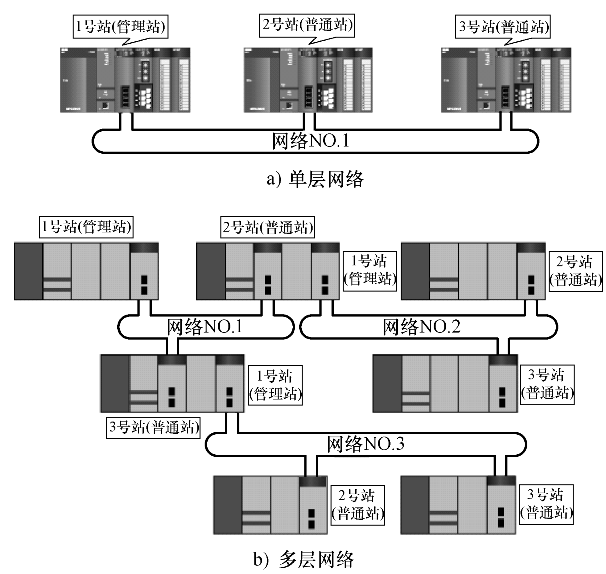


图 5-100　CC-Link 控制以太网组成

(2) 千兆现场以太网 (Field)

其组成如图 5-101 所示。

从图知，它由 1 个主（控制）站及 1 个以上的从站构成。主站主导控制数据通信的循环传输，并保存网络上所有站的循环数据。这里 Hub 也可不用，站点间可依次连接成线形

拓扑。这里主站是配置有 CC-Link IE Field 模块的 PLC。从站可用起始（即从站通信接口模块）模块加电源模块、I/O 模块组成。如图 5-102 所示用三菱的 L 型 PLC 的起始模块 LJ72GF15-T2 及其 I/O 模块构成的从站。

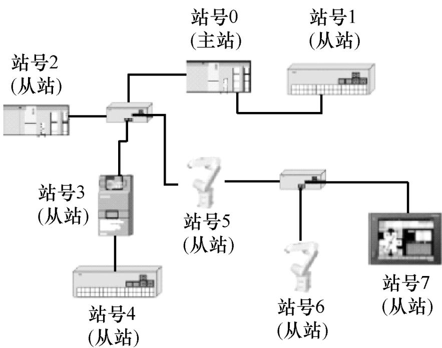


图 5-101　千兆现场以太网（Field）组成

一般讲，CC-Link IE Field 上的设备可分为控制（主）站与从站两大类。它可接入控制器、驱动器、阀等常用工业装置。通过网关，CC-Link 兼容产品也可接入网络中。通过适配器，10M/100M 的以太网设备也可接入到网络中。

主站与智能设备站之间通信通过对应地址映射实现。有位及字数据交换两种。图 5-103 所示为位数据交换。此外还有与此类似的字数据交换。

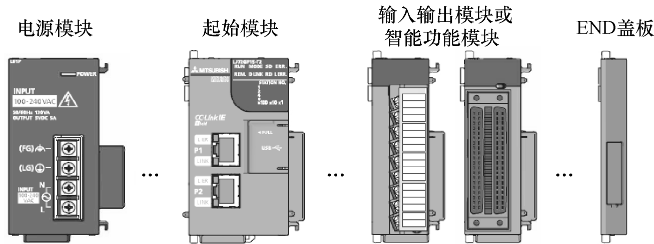


图 5-102　从站组成

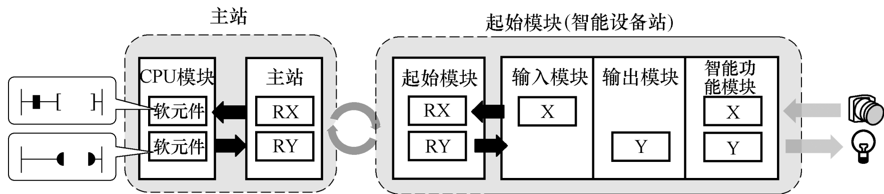


图 5-103　位数据交换

从图知，如智能设备站的按钮区控制自身的指示灯。其过程是：按钮状态通过输入模块的输入点 X 传递给起始模块的 RX，再通过以太网循环通信（解释见后），传递给主站以太网模块的 RX，进而通过 PLC IO 刷新再传递给 CPU 的软元件（具体地址与主站 RX 按以太网模块在其上安装位置有关）；这时，如果 PLC 运行图示程序，将使输出软元件的状态与输入软元件一致；再接着就是数据交换的相反过程，即 CPU 模块软输出元件（具体地址也与主站 RX 按以太网模块在其上安装位置有关）的状态通过 PLC IO 刷新传递给其上以太网模块的 RY，再进而则通过以太网循环通信把这个 RY 状态传递起始模块的 RY；再接着这起始的 RY 状态传给智能设备站的输出模块的 Y。这样过程周而复始，以实现这里的按钮对指示灯的控制。显然，这样控制从本质上与当地一样，不同的只是增加通信延迟。由于 CC-Link IE 以太网为千兆速度，通信的确定性还有保证，所以，这样

延迟完全可以接受。

2. CC-Link/IE 以太网基本功能

整合网络“CC-Link IE”不仅具有控制功能，而且还有设备管理（设定・监视）、设备保全（监视・故障检测）、数据收集（动作状态）等功能。可实现系统整体的优化。具体功能有：

（1）循环通信功能

是指在同一网络内的所有站点间按确定传输速率，利用网络共享内存，交换控制数据。三菱称之为 *N*∶*N* 的控制数据通信，其他 PLC 网络称为数据链接。循环通信的网络型共享内存容量为：位（bit）单位型共享内存最大 4KB、字（word）单位共享内存最大 256KB。这个循环通信。如图 5-104 所示，有 4 个站点可共同使用 256 字节的循环通信。各站在自己的写区发送数据，而由其他站点接收此数据。

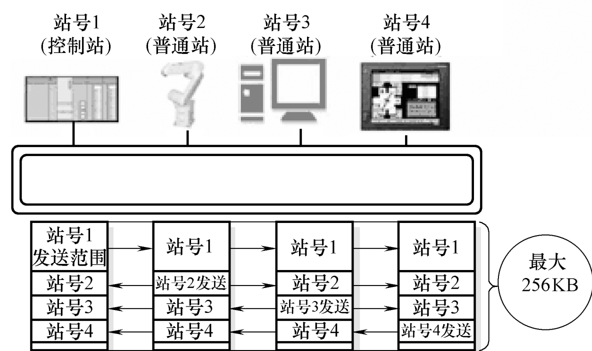


图 5-104　4 个站点循环通信

CC-Link IE 控制层网络通信速度为 1Gbit/s，用此循环通信，可实时进行各站点控制数据的更新。例如由 32 站组成的网络，某一个站用循环传输将 4KB 的控制数据发送到全部站的时间（全部站完成接收控制信息的时间）最短仅 62μs。即使有 64 个站点，这多的数据交换在 5ms 也可完成。

（2）瞬时通信功能

指任意设备之间进行点对点、非循环通信。实时性及确定性不高，但数据量可较大。通信是不规则的，但由于 CC-Link IE 对它指定有专用的带宽，所以，它不会对循环通信有所影响。此功能可使各设备可对所有其他设备进行无缝通信，而不论网络物理层的构成，仅将其视为逻辑上的单层网络。图 5-105 所示为 CC-Link IE 控制层网络瞬时通信示意。

（3）网络的高可靠性功能

具体含：

1）传输路径冗余环路功能（指控制网络）。此功能是由于 CC-Link IE 使用冗余环路的标准传输路径。各站一旦检测出异常情况，如图 5-106 所示可将异常部分切断，正常站间仍继续进行循环传输。

2）电缆不良部分检测功能。此功能是由于 CC-Link IE 的传输帧格式在基于以太网的 FCS（Frame Check Sequence）之外，在帧部分与传送数据部

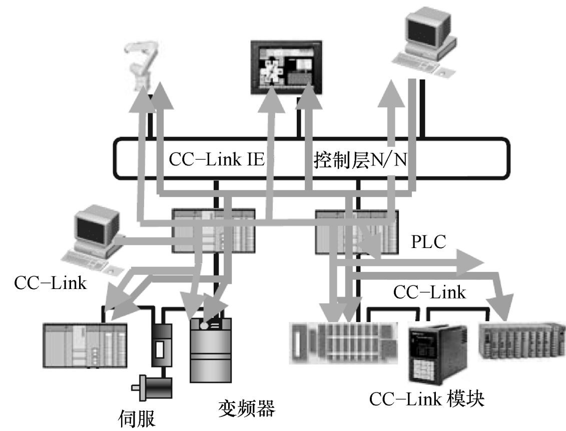


图 5-105　瞬时通信

分上新增加了错误检查编码。通过此功能，通信数据的可靠性进一步增强，如果因电缆故障而破坏了帧数据时，错误检查可只限定在首先收到错误数据信息的站，如图 5-107 所示，由此可简单检测出电缆故障部分所在。

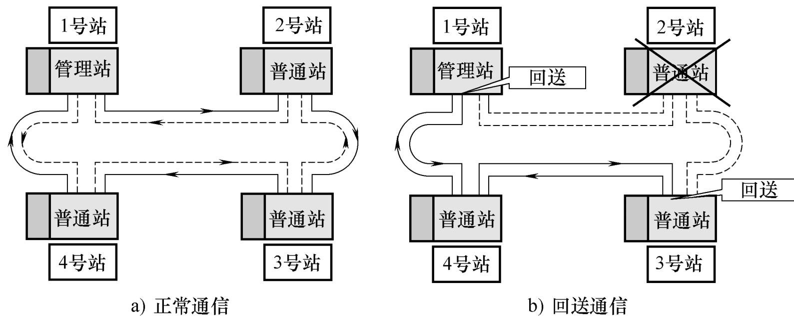


图 5-106　正常通信与回送通信

3）控制站转移功能。有了此功能，如果 CC-Link IE 控制层网络上的控制站由于某种原因发生故障时，将从普通站中选出代替控制站的站。因此即使控制站发生故障，如图 5-108 所示，正常站间也可以继续站间的循环传输。

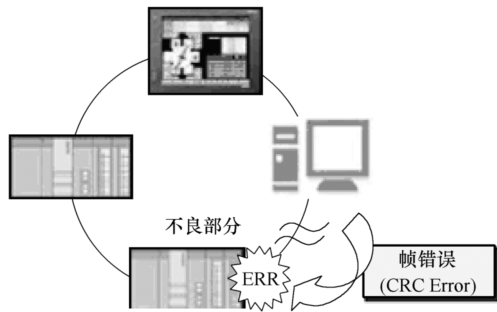


图 5-107　检测电缆故障所在

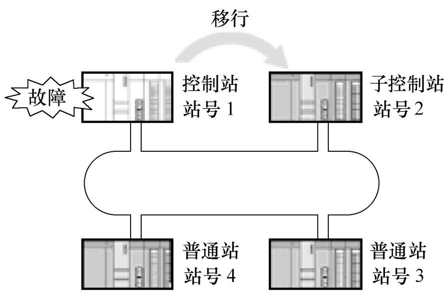


图 5-108　正常站可继续站间循环传输

3. CC-Link/IE 网络模型

CC-Link IE 控制网及现场总线网的网络模型如图 5-109 所示，分为 4 层。

底层是以太网 IEEE802.3 千兆以太网标准。这为网络的选材、安装及调试提供了方便。

数据链路层的媒体访问用周而复始地顺序传递令牌控制，拥有令牌的站点才可以发送数据。循环数据通信的确定性就是有这个令牌保证，而不是像其他工业以太网那样，靠交换机保证。

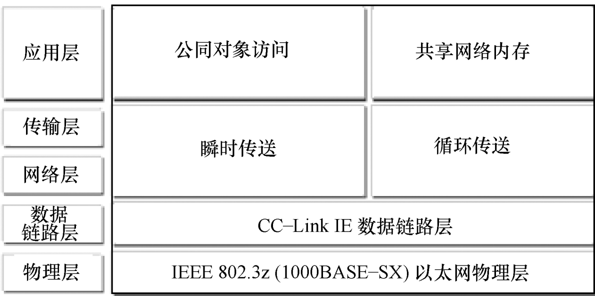


图 5-109　网络分为 4 层

数据链路层的帧格式如图 5-110 所示。除了以太网帧的头，其余数据部分包含 CC-Link IE 的帧头，之后才是 CC-Link IE 的数据。而在以太网帧头中则含有 MAC 地址等相关信息，与以太网的标准一致。正是由于它

传送的是以太网帧格式，所以，才称之为基于以太网。

网络层、传输层分别定义了瞬时通信及循环通信协议。应用层与瞬时通信及循环通信对应定义了公同对象访问及共享网络内存。前者可通过 SLMP 无缝信息协议（Seamless Message Protocol）实现网络上任何一节点对其他任意节点的访问。

图 5-110 CC-Link IE 帧格式

4. CC-Link/IE 拓扑结构

CC-Link IE 控制层网络用的是基于以太网的环路拓扑结构。其现场总线网络可使用多种拓扑结构，如图 5-111 所示。

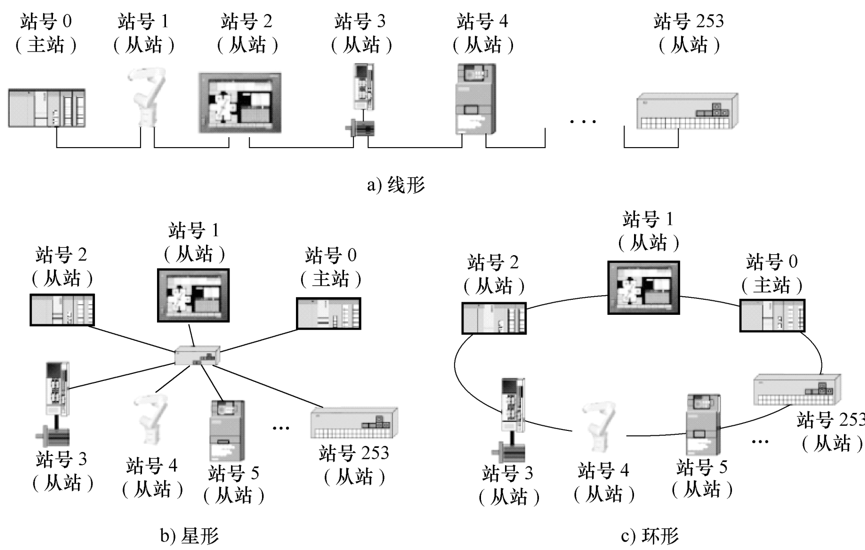


图 5-111 现场总线网拓扑结构

5. CC-Link/IE 以太网规格

CC-Link IE 整合网络目前已发布了其中的两大协议：CC-Link IE 控制网络（CC-Link IE Control）协议与 CC-Link IE 现场网络（CC-Link IE Field）协议。进一步还有运动网络协议等。其控制与现场网络主要规格见表 5-22。

表 5-22 CC-Link IE 控制与现场网络主要规格

项目 \ 类别	CC-Link IE Control	CC-Link IE Field
通信速度/(Gbit/s)	1	1
通信介质	IEEE802.3Z 多模光纤(GI)	屏蔽双绞线电缆(5e 类)
连接器	IEC61754-20LC 连接器（Duplex 连接器）	RJ45

（续）

项目＼类别	CC-Link IE Control	CC-Link IE Field
网络拓扑	环形	星形、线形（星、线可组合）、环形
每个网络最大连接台数	120	254（主从合计）
站间距/m	最大 550（使用多模光纤）	100
网络型共享内存容量/KB	最大 256	位数据：4 字数据：32

6. CC-Link/IE 以太网特点

1）CC-Link IE 基于以太网技术，实现了从信息层到现场层“一（e）网到底”的垂直整合，全面的削减了用户从工程设计、施工到维护的整体成本。如在配件上采用符合国际标准的以太网电缆或光纤、工业级 Hub 等，方便全球采购。众多设备供应商生产的标准的网络分析仪、多样的设备种类，可方便用户灵活选购。

2）1Gbit/s 的高速通信，采用周期性数据循环通信，非周期性数据瞬时通信两种通信方式，且两种通信方式享有独自的带宽，确保循环通信的实时性，确保通信的稳定性与可靠性。

3）大容量的通信数据。实时数据与非实时数据可同时存在。实时数据的交换基于分布式共享内存架构，各设备间实现了最大 256KB 的大容量网络共享内存。可共享大容量的控制信息。能简单地实现各设备间的联动与各设备的分散控制。

4）CC-Link IE 继承与发展了 CC-Link 的开放性、易使用性及丰富的 RAS（Reliability 可靠性、Availability 可使用性、Serviceability 可维护性）功能。稳定、可靠、使用简单。

5）拓扑结构灵活：现场总线网有线形、星形、环形及其相关组合等；控制层为环形拓扑，一旦检测出电缆断线或出现异常情况时，可将异常部分切断，正常站间仍继续进行循环传输。

6）在网络构成上，CC-Link IE 可以构筑单层网络（最大可连接 120 层），也可以构筑多层网络（最大可连接 239 层），使用户可以灵活的配置网络系统。通过 SLMP 通用协议实现了 CC-Link IE、CC-Link 及以太网设备之间的无缝通信，最大限度地扩展了网络设备的访问与管理功能。

7）它实时通信靠令牌传递实现。所以，联网用集线器就可以了，不需要昂贵的交换机。

8）编程简单：程序设计时只需对分布式共享内存进行读/写，不必要考虑网络拓扑结构。

5.6.2　三菱 CC-Link IE 组件及配置实例

1. CC-Link IE 网络模块

（1）主站模块

有与 Q 系列机配套的 QJ71GP21-SX、QJ71GP21S-SX（带外部电源供应端子）网络模块。还有 Q80BD-J71GP21-SX 及 Q80BD-J71GP21S-SX（带外部电源供应端子）计算机插

板，前者可与 Q 系列 PLC，后者可与计算机配套搭建 CC-Link IE 网络。这 4 个组件外观如图 5-112 所示。QJ71GP21-SX、QJ71GP21S-SX 面板外观如图 5-113 所示。

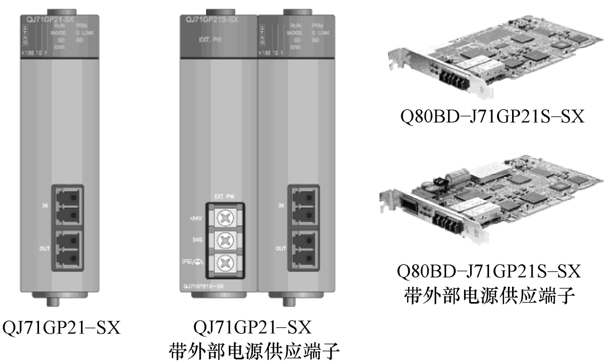


图 5-112 三菱 CC-Link IE 主站模块组件外观

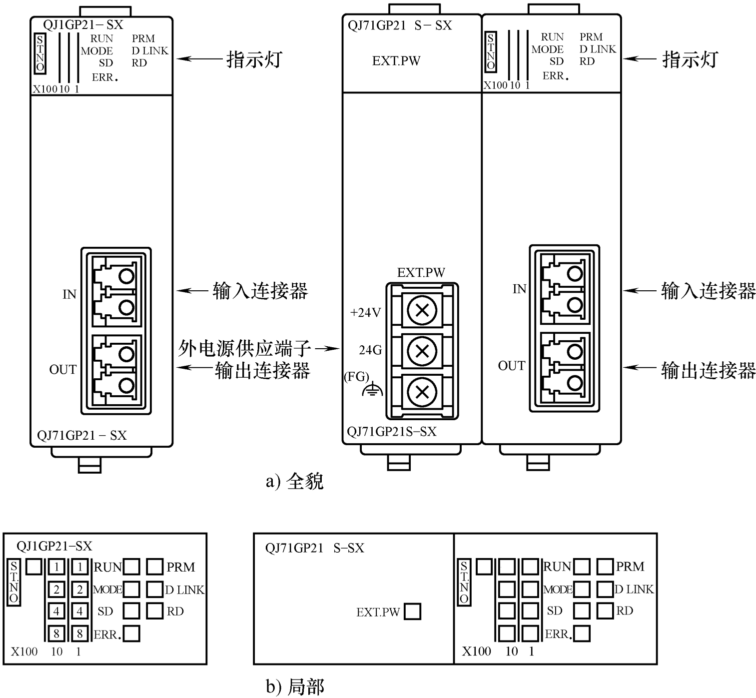


图 5-113 QJ71GP21-SX、QJ71GP21S-SX 面板外观

这里的带电源供应端子的模块目的是接如 UPS、电池等外部电源，已防止站点意外离网。两个光纤连接器，为一进、一出，如图 5-114 所示，便于直接连接环网。表 5-23 所示为 QJ71GP21-SX、QJ71GP21S-SX 规格。

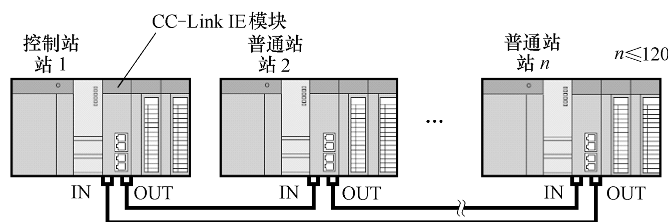


图 5-114　模块直接连网

表 5-23　QJ71GP21-SX、QJ71GP21S-SX 规格

项　　目			规　　格	
			QJ71GP21-SX	QJ71GP21S-SX
每一网络最大链接点数		LB	32K 点(32768 点,4KB)	
		LW	128K 点(131072 点,256KB)	
		LX	8K 点(8192 点,1KB)	
		LY	8K 点(8192 点,1KB)	
每一站最大链接点数		LB	16K 点(16384 点,2KB)	
		LW	16K 点(16384 点,32KB)	
		LX	8K 点(8192 点,1KB)	
		LY	8K 点(8192 点,1KB)	
瞬时传输容量			最大 1920B	
通信速率			1Gbit/s	
每一网络最大连接站数			当使用通用 QCPU 时。120 站 (其中管理站 1 站,普通站 119 站) 当使用高性能 QCPU 时,64 站 (其中管理站 1 站,普通站 63 站)	
通信介质			多模光纤	
最大网络数			239	
最大组数			32	
传送路径			双路环网	
光纤规格			1000BASE-SX(MMF)光纤	
	标准		IEC60793-2-10 Types A1a. 1(50/125μm 多模)	
	传输损耗		≤3.5(dB/km)(λ=850nm)	
	传输波段		≥500(MHz · km)(λ=850nm)	
连接器规格			全双工 LG 连接器	
	标准		IEC61764-20 Type LC 连接器	
	连接损耗		≤0.3(dB)	
	研磨面		PO(Pnysica Contact)研奥	
占用 I/O 点数			32	48

(2) 智能设备站模块

有新推出的 LJ72GF15-T2 CC-Link IE 现场总线的从站模块。具有 1Gbit/s 高速实时传送协议，用以连接三菱 L 系列机的 IO 模块，以实现主站对远程 I/O 现场设备的控制。其规格见表 5-24 所示。

表 5-24　LJ72GF15-T2 规格

项　　目	LJ72GF15-T2
传送速度	1Gbit/s
网络拓扑结构	星形拓扑、线性拓扑、星形和线性混合拓扑及环状拓扑
通信方式	确定性通信(令牌传递)
模块最大连接数量	10
通信端口	CC-Link IE Field 网络端口 ×2、USB 端口(mini 型端子) ×1
RAS 功能	网络事件记录、设备出错记录、测试、监控及出错记录保存功能
连接电缆	以太网电缆(五类或五类以上)

2. CC-Link IE 控制网络配置实例

(1) 两站点连网

本例选材来自三菱电机自动化（中国）有限公司网站中 E-learning。它有两个站点，如图 5-115 所示，1 号站位管理站，2 号站位普通站。

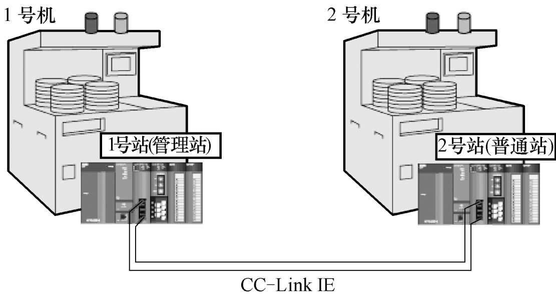


图 5-115　两站点连网

所用可编程控制器的模块构成和 I/O 分配如图 5-116 所示。

其以太网模块上有“IN”、“OUT”连接器。可用它连接光纤。一个站的“OUT”和下一站的“IN”通过光纤电缆相连。如图 5-115 所示，依次连接好“OUT”→“IN”、“OUT”→“IN”后，形成一个环。如站点多，也是类似依次连接成如图 5-117 所示的环型拓扑结构。

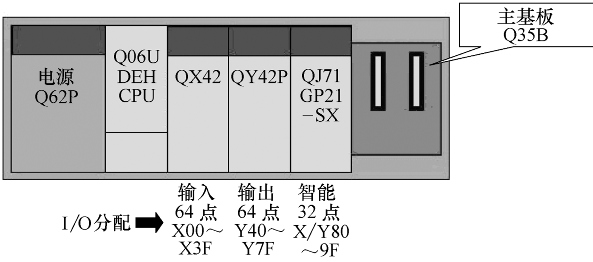


图 5-116　站点模块配置

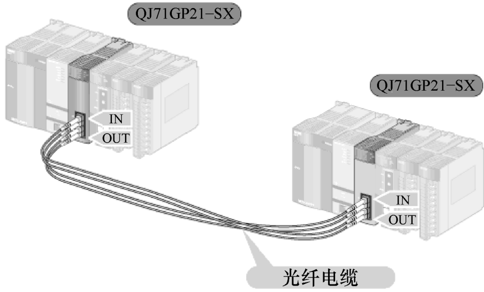


图 5-117　依次连接成环形网络

1 号站（管理站）的网络设定是：起始 I/O 号为 0080，网络号为 1，总站数为 2。组号为 0，站号为 1。2 号站（普通站）的网络设定是：起始 I/O 号为 0080，网络号为 1，总站数为 2。组号为 0，站号为 2。管理站中还要进行的通用参数分配，其设定的范围如图 5-118 所示。

	链接继电器		链接寄存器
1 号站	LB0～LBFF (256 点)	1 号站	LW0～LWFF (256 点)
2 号站	LB100～LB1FF (256 点)	2 号站	LW100～LW1FF (256 点)

图 5-118　通用参数设定的范围

为了实现通信，要在计算机上运行三菱 GX Developer 编程软件，并 PLC 联机，把上述设定下载分别给两个 PLC 站点。为了使用好链接数据，还要编写相应程序。如 2 站有如图 5-119 所示程序。

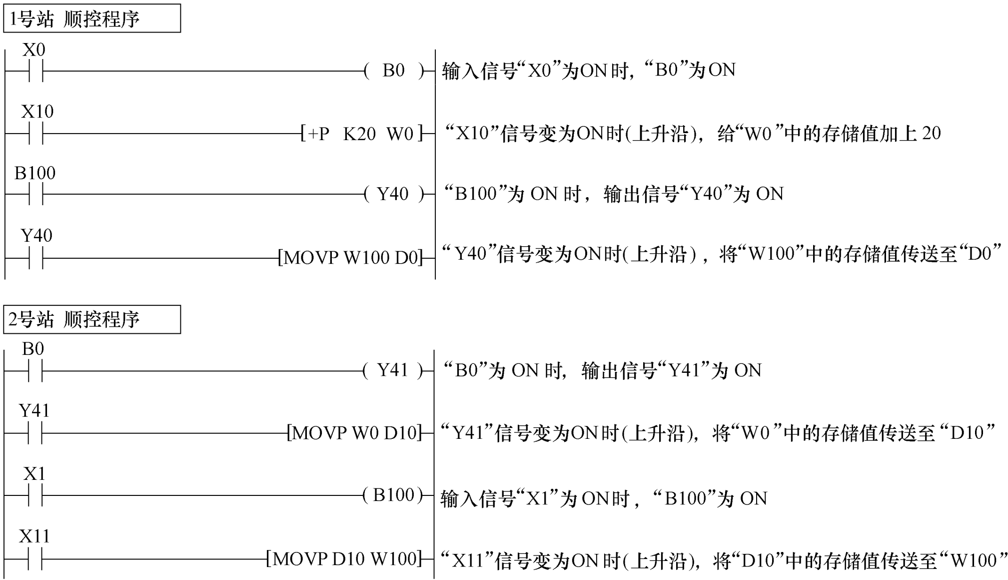


图 5-119　两站使用通信数据程序

这程序的功能是：1 号站的开关“X10”每次为 ON 时，“W0”被加上 20（数值每次增加 20）。同时 2 号站的“W0”的值也随之变化。将 1 号站的开关“X0”ON/OFF 时，线圈“B0”ON/OFF，同时 2 号站的触点“B0”随之 ON/OFF。2 号站的“B0”ON/OFF 时，线圈“Y41”ON/OFF。“Y41”变为 ON 时，“W0”的值被传送至“D10”。随着 2 号站开关“X1”的 ON/OFF，线圈“B100”ON/OFF，同时 1 号站的触点“B100”ON/OFF。随着 1 号站触点“B100”的 ON/OFF，线圈“Y40”ON/OFF。2 号站开关“X11”ON/OFF 时，上述“D10”的值被传送至“W100”。1 号站的“Y40”变为 ON 时，“W100”的值被传送至“D0”。

这些效果可通过的顺控程序动作模拟来确认上述操作执行过程中数据通信的进程。如图 5-120 所示，如点击 1 号站的“X0”、“X10”、2 号站的“X1”、“X11”各开关，都可通过指示灯、数据显示及梯形图确认数据通信的过程。点击“初始状态”按钮，则返回操作开始前的初始状态。

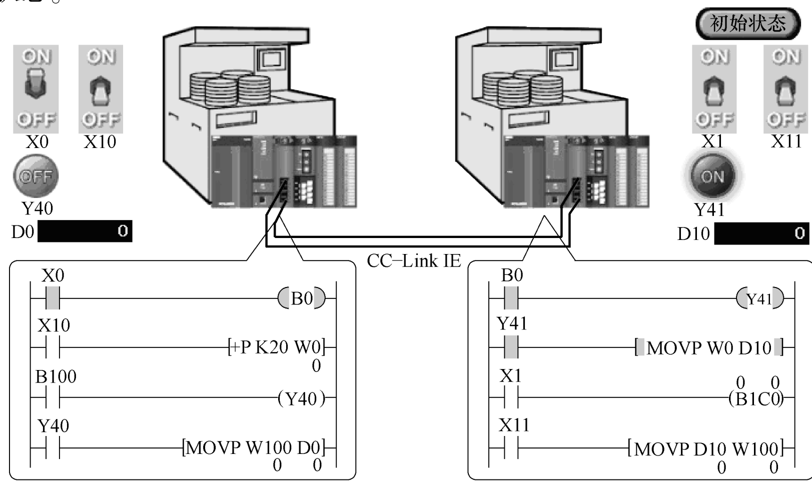


图 5-120　通信程序效果模拟

至于更多细节可登录该网站参与学习。这里略!

(2) 图 5-121 为 FPD 制造生产线的 CC-Link IE 控制层网络网络应用案例

CC-Link IE 控制层网络具有最大 256KB 的网络共享内存，可对大容量制造处方数据及各装置控制数据进行实时（如上面构成时，更新数据时间在 5ms 以内）共享。因此，各装置间共享控制情况，并各自运作协调，更易构筑高速分散的控制系统。

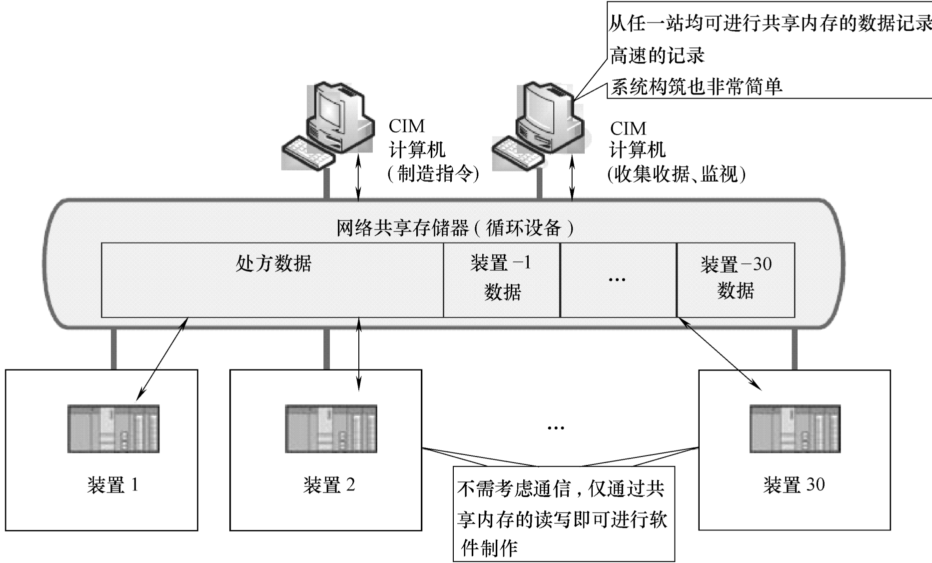


图 5-121 CC-Link IE 控制层网络网络应用案例

要指出的是，CC-Link IE 控制网还比较成熟，其他的多还在开发过程中。规范有了但实际产品还不多，或有待开发。要了解更好的应用实例也许还要稍等。

5.6.3 三菱信息网组件及其配置实例

除了 CC-Link IE 三菱还有自身的信息网，用的是以太网协议。

1. 组件

以 Q 型机为例有：QJ71WS96 Web 服务器模块及 QJ71E71-100、QJ71E71 和 QJ71E71-B2。L 型机的 CPU 还集成有以太网接口。表 5-25 所示为 QJ71E71-100、QJ71E71 和 QJ71E71-B2 模块特性。

表 5-25 QJ71E71-100、QJ71E71、QJ71E71-B2 模块特性

项目		规格				
		QJ71E71-100		QJ71E71		QJ71E71-B2
		100BASE-TX	10BASE-T	10BASE-T	10BASE5	10BASE2
传送规格	数据传送速率(Mbit/s)	100	10			
	传送方法	基带				
	最大节点-节点距离/m(ft)	—			2500 (8203)	925 (3035)
	最大段长	100(328)			500 (1641)	185 (607)
	最多的节点/连接数	级联连接，最多 2 级	级联连接，最多 4 级		100 个单元/段	30 个单元/段
	最小节点间隔/m(ft)	—			2.5(8.2)	0.5(1.6)

（续）

项　　目			规　　格				
			QJ71E71-100		QJ71E71		QJ71E71-B2
			100BASE-TX	10BASE-T	10BASE-T	10BASE5	10BASE2
发送/接收数据存储器	允许同步开启的数目		16 个连接(顺控程序可用的连接)				
	固定缓冲存储器		1k 个字 ×16				
	随机访问缓冲存储器		6k 个字 ×1				
	电子邮件	附件	6k 个字 ×1①				
		正文	960 个字 ×1		—		
占用的 I/O 点数			32 点(I/O 分配:智能)				
5V 直流电流损耗			0.50A				0.70A
噪声耐久性			根据以太网模块安装站中的电源模块规格				
绝缘电压							
绝缘电阻							
12V 直流外部功率容量(收发机)						②	
外部尺寸/mm(in)			98(3.9)(*H*)×27.4(1.1)(*W*)×90.5(3.6)(*D*)				
重量/kg			0.11		0.13		0.14

① 网络　集线器和节点之间的长度。

② 必须使用符合收发机和 AUI 电缆规格的电源，同时要考虑模块中的电压降（最高 0.8V）。

2. 协议

如图 5-122 所示，支持 TCP/IP 及 UDP/IP 协议。TCP 协议：最多可建立 16 个连接。且可同时在以太网模块中与多个缓存区通信。UDP 协议：可高速传送，但不可靠，不过通过校验提高可靠性。IP 协议：已数据报格式发送与接收数据。ARP 协议：可从 IP 地址获得以太网物理地址。ICMP 协议：可提供传送 IP 错误信息功能。FTP 协议：用于传送文件。DNS 协议：可将 IP 地址翻译成容易记忆的站名。STMP 协议：可用于传送邮件。POP3 协议：用

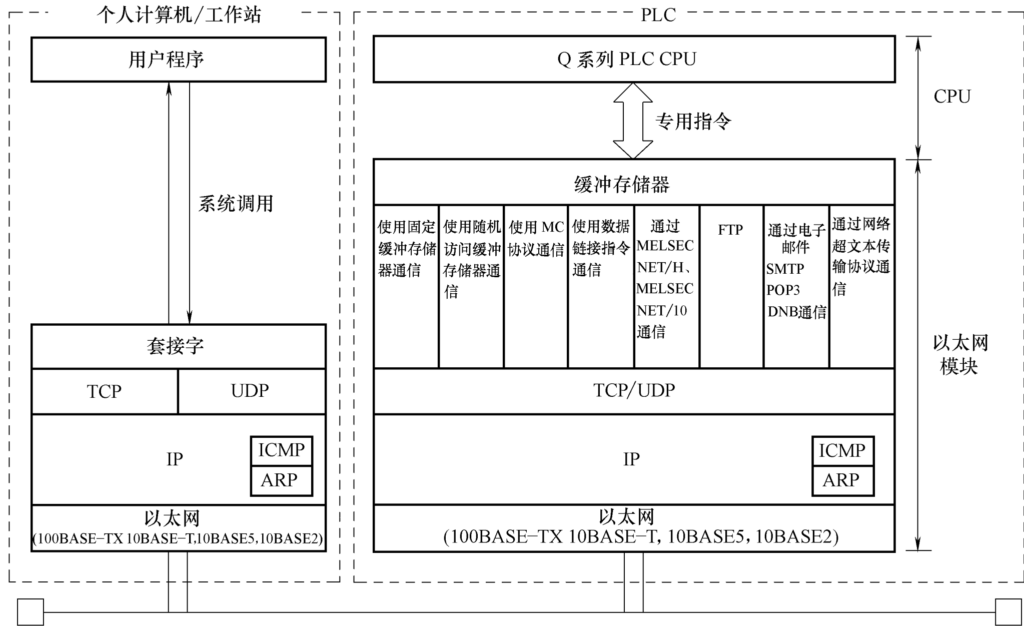


图 5-122　支持 TCP/IP、UDP/IP 协议

于邮件服务器将收到的邮件转送。HTTP 协议：用于网络数据通信。

3. 功能

（1） 电子邮件功能

通过 Internet，PLC 可向计算机发送多达 6k 字电子邮件（正文或附件）；反之，PLC 也可接收来自计算机传来的多达 6k 字电子邮件（正文或附件）。而且，还设置自动通知。只通知条件符合，PLC 还可自动发送这个邮件。

（2） 中继功能

有关站点可通过共存的以太网和三菱专有的 MELSECNET/H，MELSECNET/10 网络系统，经多重中继可以访问另外站的 PLC 站点。

（3） PLC 站点之间数据通信功能

一个 PLC 站点可使用 SEND/RECV/READ/WRITE/REQ/ZNRD/ZNWR 指令，通过以太网，把数据发送到另外站点的 PLC，或从另外站点的 PLC 接收数据。

（4） 支持 TCP/IP 标准协议 FTP（文件传送协议）的服务器功能

可使用 FTP 命令，以文件为单位读/写 QCPU 文件，因而可通过计算机按照需要管理 QCPU 文件。

（5） Web 功能

使用 Web 浏览器通过因特网监视远处的 Q 系列 CPU；可收集或更新 PLC 数据；可以监视 CPU 模块操作；可以进行 CPU 模块的状态控制。此外，增加 Web 服务器（运行三菱提供的 Web Server 软件的计算机），还可增加更多的功能：如创建复杂的屏幕；减少以太网模块上的负荷；分离以太网线路；等等。要指出的是不是所有以太网模块有此功能，如 QJ71E71-100、QJ71E71-B5 及 QJ71E71-B2 以太网接口模块才有此功能。

4. 配置实例

（1） 用 QJ71E71-100 配置以太网

用该模块按网络集线器按 10BASE-T 或 100BASE-TX 标准连接。图 5-123 所示为使用 100BASE-TX 标准集线器连接。

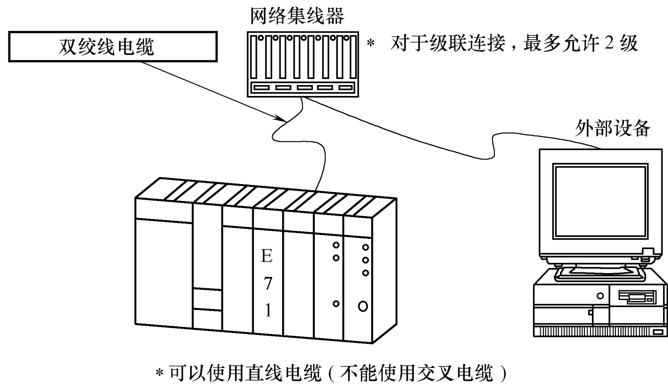


图 5-123 使用 100BASE-TX 标准集线器连接

除了接线，还要通过编程软件 GX Developer 设置以太网模块参数。具体略。

（2）通过因特网进行访问具有 Web 功能模块系统配置

图5-124所示即为这个配置实例。

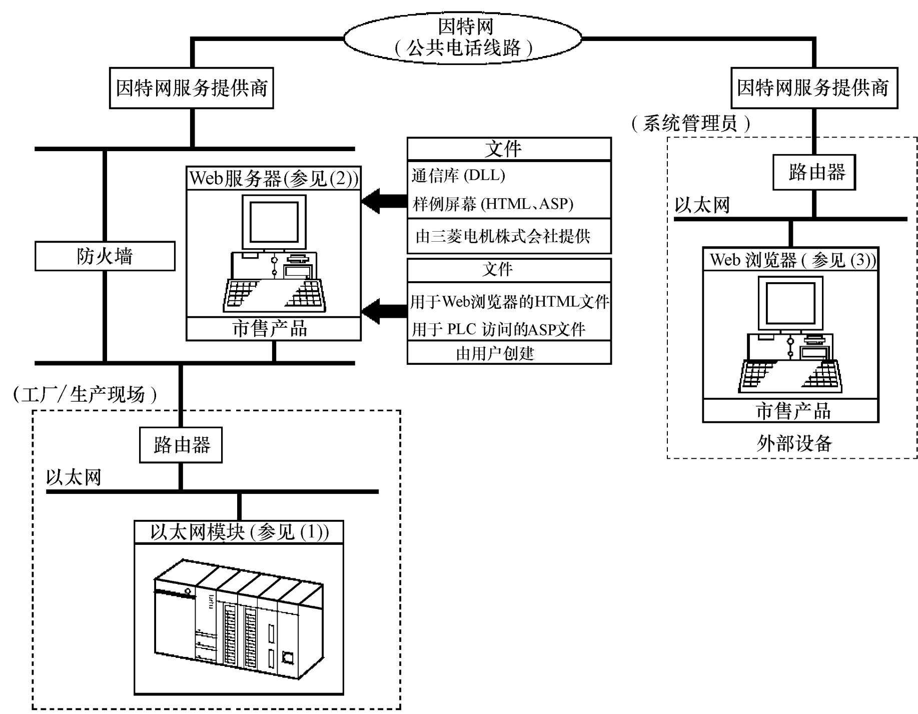


图5-124 使用Web功能配置实例

图中参见（1）为上述具有Web功能的以太网模块。参见（2）为Web服务器，其上要安装与运行相应软件。参见（3）为Web浏览器，用以在远程通过因特网访问Web服务器。由于后者与PLC是实时连网的，所以，也间接地访问了PLC。当然如果不用Web服务器，远程Web也是可以访问PLC的。只是功能略少。

参 考 文 献

［1］ Andred S Tanenbaum. 计算机网络［M］. 潘爱民，译. 4 版. 北京：清华大学出版社，2004.
［2］ 崔坚. 西门子工业网络通信指南：上册，下册［M］. 北京：机械工业出版社，2004.
［3］ 谢希仁. 计算机网络［M］. 5 版. 北京：电子工业出版社，2008.
［4］ 宋伯生. 机床电器及电控制器［M］. 北京：中国劳动出版社，1990.
［5］ 宋伯生. 可编程控制器［M］. 北京：中国劳动出版社，1993.
［6］ 宋伯生. 可编程控制器配置·编程·联网［M］. 北京：中国劳动出版社，1998.
［7］ 宋伯生. PLC 编程理论、算法及技巧［M］. 2 版. 北京：机械工业出版社，2009.
［8］ 宋伯生. PLC 编程实用指南［M］. 北京：机械工业出版社，2007.
［9］ 宋伯生，陈东旭. PLC 应用及实验教程［M］. 北京：机械工业出版社，2006.
［10］ 宋伯生. PLC 系统配置及软件编程［M］. 北京：中国电力出版社，2007.

后　记

编写本书酝酿了好久。在多年前就起步了。但由于种种原因，拖到今天。好在本书编辑罗莉一再鼓励与支持下，今天终于与读者见面了。为此，我衷心对罗莉同志深表谢意！

在编写本书过程中，在 AB、西门子、OMRON、三菱、和利时等公司的网站上，下载与阅读了大量相关手册、样品说明以及视频材料，为本书的编写提供了宝贵帮助。没有这些网站，没有当今互联网发展，要编写好本书是不可能的。所以说“本书是当今互联网的幸运儿”一点也不过分！读者不妨在互联网上搜索这些网站，也登录看看，一定也会受益不浅的。

在本书编写过程中得到了沈阳鹭岛、沈阳旭风公司很多同仁的参与与帮助。特别是盛阳、马文焕、宋成功、高维江、王德春、周建等工程师还提供了本书部分章节的素材，并仔细审读了有关章节的书稿。对本书的顺利完稿功不可没。在此，作者对他们深表谢意！

编写本书还得到了沈阳鹭岛公司总经理张波先生、沈阳旭风电子公司总经理陈东旭先生的大力支持与鼓励，在此特向他们表示深深谢意！

在我的书稿最后定稿中，史春卿、姜海涛、宋巍、姜汝冰、宋云起等也参与了部分工作，在此，也顺便向他们致以谢意！

宋伯生　2010 年 12 月　于沈阳

PLC 系列图书书目

序号	书名	书号	定价	出版时间
1	图解西门子 TDC 与 S7-300/400PLC	978-7-32704-2	58	201103
2	例说西门子 S7-300/400 系列 PLC	978-7-33103-2	48	201103
3	图解西门子 S7-1200PLC 入门到实践	978-7-31816-3	50	201101
4	LOGO！控制器实训教程(1CD)	978-7-29756-7	39	201006
5	西门子 S7 系列 PLC 的应用与维护	978-7-23439-5	50	200912
6	西门子 S7-200/300/400PLC 基础与应用技术	978-7-25898-8	34	200907
7	S7-200PLC 原理与实用开发指南	978-7-25157-6	39	200901
8	S7-200PLC 编程设计与案例分析	978-7-28311-9	68	201001
9	S7-300/400PLC 编程设计与案例分析	978-7-27976-1	79	201001
10	S7-300/400PLC 梯形图与语句表编程	978-7-26146-9	40	200904
11	S7-300/400PLC 原理与实用开发指南	978-7-24871-2	36	200810
12	S7-300/400PLC 实用开发指南	978-7-20286-8	50	200802
13	松下 PLC 编程与应用	978-7-27217-5	40	201008
14	PLC 及 I/O 设备应用教程	978-7-27870-2	33	200909
15	三菱 PLC 编程技术及工程案例精选	978-7-32700-4	39.8	201101
16	三菱 Q 系列 PLC 原理与应用设计	978-7-28475-8	66	201001
17	三菱可编程序控制器应用技术	978-7-29592-1	33	201004
18	三菱 PLC 基础与系统设计	978-7-27268-7	40	200908
19	三菱 FX 系列 PLC 设计与开发——原理、应用与实训	978-7-26538-2	40	201008
20	施耐德电气可编程序控制器原理及应用(1CD)	978-7-19576-4	55	200807
21	PLC 编程理论、算法及技巧(第 2 版)(1CD)	978-7-26319-7	88	201001
22	PLC 编程实用指南(1CD)	978-7-19297-8	68	200901
23	电器控制与 PLC(西门子 S7-300 机型)	978-7-29752-9	40	201006
24	可编程序控制器与工业现场总线(1CD)	978-7-29884-7	49	201005
25	可编程序控制器原理及应用技巧	978-7-28716-2	40	201004
26	可编程序控制器选用与系统设计实例	978-7-29421-4	49	201001
27	可编程序控制器选择、设计与维护	978-7-11084-2	26	200802
28	可编程序控制器原理、应用与实训	978-7-22894-3	26	200906
29	可编程序控制器原理及应用(第 3 版)	978-7-27774-3	50	200909
30	电气控制与可编程序控制器的原理及应用	978-7-14478-6	43	200807
31	可编程序控制器与工业自动化系统(1CD)	978-7-18054-8	36	200807
32	电器-PLC 控制技术及应用	978-7-20652-1	33	200806
33	变频器、可编程序控制器及触摸屏综合应用技术实操指导书(第 2 版)	978-7-30672-6	44	201008
34	机电控制系统原理及工程应用实操指导书	978-7-31227-7	30	201009

图书零售：

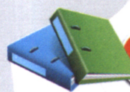
网上订购：中国科技金书网
（机械工业出版社旗下大型科技图书网站）
网址：www. golden-book. com
E-mail：service@ golden-book. com
电话订购：010-68993821　　010-88379639/9641/9643
传真订购：010-68990188
邮局汇款：
地址：北京市 100037 信箱 30 分箱
收款人：网络销售部
邮编：100037
银行转账：
户名：北京百万庄图书大厦有限公司
帐号：808516091908091001
开户行：中国银行北京百万庄支行

图书团购：

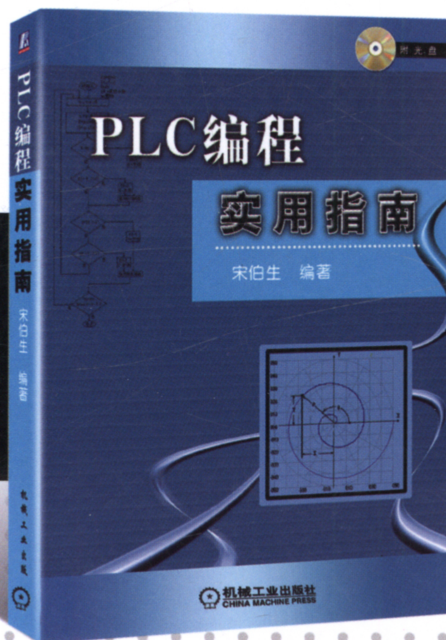
联系人：李红勇
电话：010-88379766
Email：dgdzcmp@ sina. com

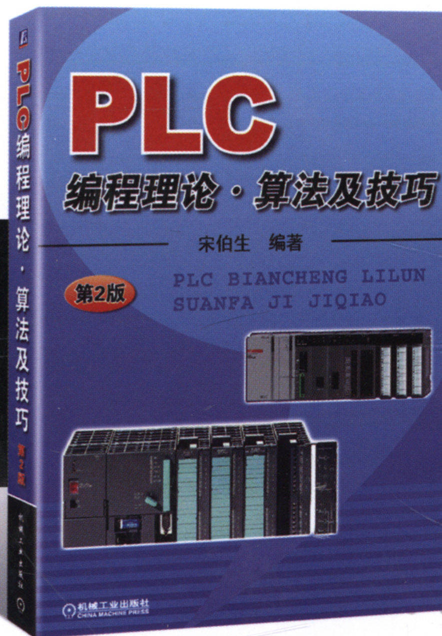
图书写作与内容咨询：

电知：010-88379762　传真：010-68326336
联系人：罗莉
网址：www. cmpbook. com
E-mail：cmpluoli@ 163. com
地址：北京市西城区百万庄大街 22 号
机械工业出版社　电工电子分社
邮编：100037



即将推出第2版





上架指导：工业技术／电气技术／PLC

◎ 策划：罗莉／封面设计：陈沛

地址：北京市百万庄大街22号
电话服务
社服务中心：(010)88361066
销售一部：(010)68326294
销售二部：(010)88379649
读者购书热线：(010)88379203

邮政编码：100037
网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com
封面无防伪标均为盗版

ISBN 978-7-111-34132-1
定价：69.80元

